Index

Preface

Tokai University 75th Anniversary Memorial International Cybersecurity Symposium was cohosted by the Strategic Peace and International Affairs Research Institute of Tokai University (SPIRIT) and the Information Security Institute of Lomonosov Moscow State University (IISI) on December 1, 2017. Representing the Japanese government were Mr. Yoshihide Suga, Chief Cabinet Secretary and the person with ultimate responsibility for cybersecurity strategy in Japan, Mr. Masato Otaka, Ambassador in Charge of Cyber Policy and Deputy Director-General of Foreign Policy Bureau, Ministry of Foreign Affairs, and Mr. Ikuo Misumi, Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity, Cabinet Secretariat (position at the time). In attendance on the Russian side were H.E. Mr. Evgeny V. Afanasiev, Ambassador of the Russian Federation to Japan (position at the time), Mr. Vladislav P. Sherstyuk, Director, Information Security Institute, Lomonosov Moscow State University and Advisor of the Secretary of the Security Council of Russian Federation, and Mr. Anatoly Streltsov, Vice Director, Information Security Institute, Lomonosov Moscow State University. With the United Kingdom also a major player in the cyber world, a British officer in charge of Russia, from the International Institute for Strategic Studies (IISS) was scheduled to attend but a sudden illness forced him to withdraw. Instead, Mr. David Ellis, Chief Minister, British Embassy, attended the symposium and delivered an opening speech. It was our belief that along with the cooperative relationship between SPIRIT and IISI, which has a long track record in the field of cybersecurity research, the participation by a British intelligence officer who had been stationed in Moscow for many years, would lead to the clear identification of differences in approach toward cybersecurity issues of the two research institutes. Given the current tense relationship between the United Kingdom and Russia, I would like to express my respect and appreciation to Moscow State University for their positive stance toward this symposium involving the three countries of Japan, Russia and the United Kingdom.

I cannot help but feel that Dr. Shigeyoshi Matsumae, the founder of Tokai University, provided a clear path for SPIRIT to following in the future as he devoted much effort into exchanges between universities and organizations in Japan, the Soviet Union (now Russia), and Eastern European countries, where information exchanges were scarce during the Cold War. At the end of the symposium, Director Sherstyuk presented Chancellor Kiyoshi Yamada a proposal on cybersecurity titled "Concept of the draft UN Convention (Concept of secure functioning and development of the Internet) The proposal states that we "recognize the need to mobilize efforts of the international community to prevent using the Internet for purposes contrary to the UN Charter", "recognize the need for new international arrangements to harmonize interaction and the role of the state, global ICT companies, enterprises, responsible for the development of standards, technologies and communications networks" and "emphasize that no single State or a group of States shall have the right to cause interference to the Internet functioning, establish Internet norms and rules at its sole discretion, use mass surveillance, try to manipulate foreign public opinion or destabilize situation in sovereign States". This is a proposal from a university research institute in Russia, where the Security Council of Russia, chaired by President Vladimir Putin, coordinates all strategies and doctrine relating to Russian security. The significance of IISI attending and making recommendations at this symposium should be duly noted as this organization has a great influence on the Security Council of Russia.

Symposium discussions threw light on the evident differences surrounding the concept of "sovereign state" between Japan and Russia. In his contribution to the symposium booklet, the moderator of the symposium, Ichiyo Ishikawa, Senior Commentator and Former Chief of NHK's Moscow Bureau, provided an insight into this: "Security in Russia includes not only military, political and economic aspects, but also cultural and historical traditions, education and science, and the environment. Using the Russian concept, there are relatively few true sovereign states in the world. Obviously, European countries are not true sovereign states because they have ceded political and economic sovereignty to the EU; likewise Japan, which depends so much on the United States for its defense in accordance with the Japan-US Security Treaty, may not be a true sovereign state from the Russian perspective. As Russia wants to be a true sovereign state with its own decision-making authority, security in cyberspace therefore poses a major problem for it. "Bad" Western influences from the borderless Internet could undermine the Russian state, and conversely, Russia could find itself cut off from the Internet infrastructure, which is controlled by the United States."

With regards to this particular point, cyber experts in Japan have pointed out concern over manipulation conducted via Russian and Chinese influence operations. In the leadup to the Olympic and Paralympic Games Tokyo 2020, in order to strengthen its ability to cope with cyberattacks, the Japanese government revised its Basic Act on Cybersecurity at an extraordinary session of the Diet last year. Preparations for the establishment of the Cyber Security Council, a public-private partnership where the national government, local governments, key infrastructure operators, cyber operators and educational institutions work together and share information, are already underway. Toshio Nawa, senior analyst at Cyber Defense Institute and a leading authority on cybersecurity measures points out that those involved in cybersecurity measures in Europe and the United States are keenly interested in influence operations such as the suspected involvement of Russia in the 2016 US presidential election and the utilization of big data to collect huge volumes of personal information and internal information of large organizations, something which China is reported to be actively working on. Often a flow-on effect of tensions between nations outside cyberspace, this type of cyberattack is referred to as a "hybrid threat", where one nation conducts a cyberattack on another, threatens the other nation, and tries to shake the other party up for political purpose. (From interview on cybersecurity measures; Page 13, Morning edition, January 17, 2019, Yomiuri Shimbun)

The situation has drastically changed since this cybersecurity symposium was held in December 2017. The conflict between the US and China which started out as a trade war has turned into a new Cold War, with both nations vying over who will rule the world in the near future and shows signs of becoming a head-on collision as both nations struggle for supremacy in the area of high-tech technology. In response to the changes we have seen, Japanese media have started to run more articles and TV programs on cybersecurity, but many of these tend to sensationally deal with security issues. At the symposium, Ikuo Misumi, Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity, Cabinet Secretariat (position at the time) and the person in charge of actual operations in this area for the government, pointed out that "cyberspace is an artificial space built by private investment, not by the government, and investment in cybersecurity measures should not be seen as an unavoidable cost to be borne, but rather as a value-generating investment." This insight should be more fully shared. Presently, there is a large gap between Japan, which attaches importance to the values of freedom and independence just like its ally the United States, and Russia and China, authoritarian regimes that bring state sovereignty to the forefront, when it comes to basic perceptions. In addition, we should be very concerned about both the lack of consensus between the ruling and opposition parties when revisions of the Basic Act on Cybersecurity were discussed at the extraordinary session of the Diet last year, and the low level of risk awareness on the part of

business managers in the areas of cybersecurity measures. At Tokai University, we believe that we need to establish a unique research and education system that further drives the founding spirit of the university, namely "integration of literature and science". At the same time, there is an urgent need for us to collaborate with external professional institutions, telecommunications infrastructure companies, and so on.

To compile this first SPIRIT booklet, the proposal put forward by IISI was included at the beginning of the symposium record as we thought it important to recognize the differences in "viewpoint" between Japan and Russia with regards to cybersecurity and to understand the significance of those differences. Also, in order to further understand the Japanese government's basic philosophy toward cybersecurity, Ikuo Misumi, Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity, Cabinet Secretariat (position at the time), was asked to provide a contribution based on discussions held at the symposium. Keiko Kono, a researcher at the National Institute for Defense Studies, and Yu Koizumi, a special researcher at the Institute for Future Engineering, who provided valuable opinions as commentators at the symposium, were also asked to provide contributions on problems that were clarified at the symposium.

In order for the expansion of cyberspace to contribute, not only to the field of national security, but also to improving the everyday life of people across the world and production systems, it is important that differences be clarified and a path for cooperation be explored accordingly. I sincerely hope that this booklet can contribute in some small way to achieving this.

Concept of the draft UN Convention:
Concept of secure functioning and development of the Internet

General provisions

Development of the Internet is of great importance for the humanity.

Development of technologies, services and businesses in the Internet creates new challenges for individuals, societies and States.

Internet has enabled the progress in the development of scientific knowledge, education, medicine, economy and other areas.

Proper functioning of the Internet became of significant importance for any State, its population and economy.

Currently we lack an open and transparent system of Internet governance.

We distinguish issues related to day-to-day technical and operational activity and issues related to governments' activity and their roles in carrying out their commitments in international public policy issues, pertaining to the Internet, according to Resolution 2011/16 of 26 July 2011 of the United Nations Economic and Social Council (ECOSOC).

We underline the importance of security, continuity and stability of the Internet and the need to protect the Internet from possible threats and vulnerabilities.

We affirm the need for a common understanding of the issues of Internet security, and for further cooperation at the national and international levels.

According to the UNGA Resolutions A/RES/70/237 of 23 December 2015 "Developments in the field of information and telecommunications in the context of international security" and A/RES/70/125 of 16 December 2015 "Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society" we encourage UN Member States to promote multilateral consideration of existing and potential threats in the field of information security.

We note the need to ensure a proper balance between law enforcement and respect for fundamental human rights as provided in the 1966 International Covenant on Civil and Political Rights as well as in other international human right treaties, which recognize the right of everyone for freedom to hold opinions without interference and the right to freedom of expression including freedom to seek, receive and impart all kinds of information and ideas, regardless of frontiers.

We reaffirm the need to respect, protect and ensure fundamental human rights and to recognize their importance for economic and social development, ensuring equal respect for and enforcement of all human rights, in particular the right to freedom of expression, the right to privacy, the right to receive information, anonymity, personal data protection online and offline, and other relevant human rights and freedoms.

We recognize the need to mobilize efforts of the international community to prevent using the Internet for purposes contrary to the UN Charter.

We recognize the need for new international arrangements to harmonize interaction and the role of States, global ICT companies, enterprises, responsible for the development of standards, technologies and communications networks.

We emphasize that no single State or a group of States shall have the right to cause interference to the Internet functioning, establish Internet norms and rules at its sole discretion, use mass surveillance, try to manipulate foreign public opinion or destabilize situation in sovereign States.

We affirm the importance of the Tunis Agenda for the Information Society (paragraphs 35-38, 51, 52, 69) that identified the role of all stakeholders in the Internet governance process and, inter alia, recognized that policy authority for Internet-related public policy issues is the sovereign right of States.

Purposes of Concept

Facilitate further development and improve security of the Internet, guarantee rights and freedoms of users.

Establish equitable international cooperation in the Internet governance.

Facilitate adoption and strengthening of measures towards a more effective and efficient Internet governance through improvement of national measures and international cooperation.

General principles of Internet governance

Internet governance is an open democratic process based on commonly recognized principles and norms of international law, oriented to people's needs, protection of their rights and freedoms, including personal data protection.

Internet governance shall not be subject to any unilateral political restrictions or commercial interests.

Internet governance is aimed at:

harmonization of national and international norms and standards, coordinated interaction at all levels of governance taking into account the right of each State to govern national Internet segment;

equal distribution of powers of one State to control the Internet governance systems between all States and, if necessary, other international entities;

establishment of international legal and organizational frameworks for Internet governance;

ensuring security, continuity, stability and robustness of Internet.

Principles of State behavior in the Internet governance

States have equal rights and responsibilities for international Internet-related public policy issues.

Access to Internet shall not be used by States as a tool to influence other States.

States shall refrain from actions to limit operation of and/or access to the Internet on the territory of other States.

States shall recognize the principles of equitability in the Internet governance as well as the sovereign rights of States to regulate national Internet segments.

States shall ensure safety, integrity, continuity, stability, robustness and security of national Internet segments, including functioning of critical infrastructure components of national Internet segments.

States shall respect, protect and ensure fundamental human rights and recognize their importance for social and economic development, ensuring equal respect and implementation of all human rights, particularly the right to freedom of expression, the right to privacy, the right to receive information, anonymity, protection of personal data both online and offline.

States shall govern the Internet on basis of sovereign equality, recognition of network sovereignty, sustainable development, protection from cross-border influence, ensuring security and reinforcing measures for secure functioning of the Internet.

States retain their national sovereignty over the information sphere of the Internet, guarantee protection of citizens within their jurisdictions , ensure governance, strategic robustness and protection of national Internet segments.

States, with balanced participation of stakeholders at the national level, have the right to independently allocate, assign and withdraw numbering and naming resources, maintain Internet addressing and identification, support the operation, monitor and develop the national Internet segment.

States follow principles of cooperation and mutual assistance, contribute to the development and application of international standards in order to create such an environment where users can use relevant services anywhere in the world, regardless of the applicable technology.

States shall designate national organizations responsible for national Internet segment governance in accordance with national laws. States encourage the establishment of critical Internet infrastructure components on their territories.

States ensure stable functioning of the Internet and stable access of users to its services.

States encourage international cooperation for better Internet governance at the international level, on basis of equitable participation of global community with balanced participation of stakeholders.

Principles of international cooperation in Internet governance

Development, adoption and monitoring over implementation of rules for ensuring stable functioning of Critical Internet Infrastructure shall be performed by Authorized International Organizations.

Internet governance based on equitable participation of global community implies separation of governance process into several functions as described below, and these functions should be performed by distinct organizations:

constitutive functions, such as development and adoption of policies, rules, procedures, standards and other norms that regulate relations arising during Internet governance process;

enforcement functions not related to the day-to-day governance of critical infrastructure – these include decision-making functions to create and allocate critical resources between different parties, as well as dispute resolution;

enforcement functions related to the day-to-day governance of critical infrastructure – these include implementation of adopted decisions on the allotment/allocation of critical resources, as well as management of critical resources and monitoring the operation of critical infrastructure;

functions to operate Critical Internet Infrastructure.

Constitutive and enforcement functions related to Internet governance are performed by organizations with international status which guarantees their independence from jurisdiction of any State.

Organizations empowered to manage Critical Internet Infrastructure perform their work based on contracts with Authorized International Organization, and such contracts are regularly reviewed.

Each function has two levels of governance, i.e. international and national, and Internet governance process is based on coordinated interaction of these governance levels, taking into account the right of sovereign State to regulate infrastructure at the national level.

Authorized International Organizations that govern the Internet perform allocation and, if the consent of concerned States is obtained, re-allocation of numbering, identification, addressing and naming (domain names) resources in an open and mutually agreed manner for their further management within national Internet segments of States.

Authorized international organizations ensure stable functioning of the Internet and access of users to Internet services, while States shall implement decisions of the relevant Authorized International Organizations.

Authorized International Organizations develop, implement and monitor the application of rules and standards aimed to ensure decentralization of Critical Internet Infrastructure governance, security and stable functioning of critical infrastructure of national Internet segments and of the Internet as a whole.

Principles of collaboration and assistance

States should strengthen collaboration to ensure integrity, reliable functioning and security of national Internet segments, to establish direct relations for Internet traffic transit and to develop Internet basic infrastructure.

States pursue policies aimed at meeting public requirements with respect to Internet access and use, and assist in promoting the operation and development of the Internet, including through international cooperation mechanisms.

States consider providing wide technical assistance to each other based on corresponding requests, in particular to developing countries, in connection with their corresponding Internet development plans and programs, improving Internet security and ensuring rights and freedoms for its users, including material assistance, training and mutual exchange of relevant experiences and

expertise – these measures aimed to promote international cooperation between States.

States should intensify their efforts to maximize efficiency of practical and training events within international and regional organizations and in the frameworks of other relevant bilateral and multilateral agreements or arrangements.

States consider opportunities to assist each other, upon request, in the analysis, studies and developments of the Internet, improvement of the Internet security and ensuring users' rights and freedoms in order to develop strategies and plans in these areas with participation of competent authorities and the public.

Annex

Terminology

Information and communication technologies (ICTs) are the processes, methods of searching, collecting, storing, processing, provision, and dissemination of information, as well as means for implementation of such processes and methods.

Information and telecommunication network is the technological system intended to transmit information over the links, providing access to information by means of electronic equipment.

Internet is the global information and technological network connecting information systems and telecommunication networks of different countries through the global addressing space. The Internet is based on a set of Internet protocols and data transmission protocol, and provides opportunity to implement different forms of communication including posting of information for the general public.

Critical Internet Infrastructure is the integral part of the information infrastructure, which is a combination of networks, systems and resources of the Internet, operability of which could have significant impact on the integrity, continuity, stability, robustness and security of the information infrastructure within national Internet segments.

Internet governance is the process of development and application by Governments and other stakeholders, within their respective roles and responsibilities, of common principles, norms, rules, decision-making procedures, programs and recommendations that shape conditions for the evolution and use of the Internet.

Universal model of the Internet governance is the concept of the unified approach for all stakeholders, according to their roles and responsibilities, to establish the Internet governance process, applicable for any area of the Internet governance and allowing establishment of mechanisms for resolving any issues related to these areas.

Stakeholders are States, private sector, civil society, scientific and technical communities, intergovernmental and international organizations, participating in the Internet governance process and performing their relevant roles and responsibilities in this process.

Information infrastructure is a set of technical means, systems and resources that generate, shape, transform, transmit, use and store the information.

Network sovereignty is the ability of unconditional implementation of State authorities related to information infrastructure in the national Internet segment, which the State possesses by virtue of its sovereignty and which it executes to implement sovereign power.

National Internet segment is a set of information and communication networks, systems and resources of Internet, located on the State territory and duly registered according to the domestic legislation of the State, as well as national domain zone and resources referred to national Internet segments of States within the frameworks of the relevant international treaties.

National domain zone is the area of hierarchical Internet domain name space, identified by unique domain name, allocated to a specific country and congruent with the international country code.

Domain name is a set of characters formed according to international Internet addressing rules, used to address an Internet information resource and corresponding to a particular network address.

Tokai University 75th Anniversary Memorial International Cyber Security Symposium

Organized by:
Strategic Peace and International Affairs Research Institute of Tokai University,
Information Security Institute of Lomonosov Moscow State University

Sponsored by:
The Sasakawa Peace Foundation, Nishikata Foundation

Date & Time: December 1st, 2017 (Friday) 12:30 – 17:00
Venue: The Tokai University Club, Kasumigaseki Building 35th Floor - Room "Asahi"
Languages: Japanese-Russian simultaneous interpretation
Facilitator Naoto Yoshikawa, Vice-Chancellor, Tokai University

Opening Speeches: (12:30 – 13:00)
-Yoshihide Suga, Chief Cabinet Secretary, Government of Japan
-Evgeny Afananasiev, Ambassador of the Russian Federation to Japan
-David Ellis, Chief Minister, British Embassy

Part I: Keynote Speeches: (13:00 – 14:00) Cyber Security Dialogue in Global Paradigm Shift
-Yoshimasa Suenobu (Director, Strategic Peace and International Affairs Research Institute of Tokai University) - Backgrounds and aims of the symposium
-Vladislav P. Sherstyuk (Director, Information Security Institute, Lomonosov
-Moscow State University, Advisor of the Secretary of the Security Council of Russian Federation)
-Masato Otaka (Ambassador in charge of Cyber Policy and Deputy Director-General of Foreign Policy Bureau, Government of Japan)

Part II: Presentations and Panel discussions: (14:30 – 16:30)
How information technologies contribute to socio-economic development and Quality of Life?
Moderator
-Ichiyo Ishikawa (Senior Commentator, Former Chief of Moscow Bureau, NHK)
Presenters:
-Ikuo Misumi (Councillor, Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity, Cabinet Secretariat, Government of Japan)
-Anatoly Streltsov (Vice Director, Information Security Institute, Lomonosov Moscow State University)
-Takuo Nakajima (Chief, Information Education Center, Tokai University)
-Pavel Karasev (Information Security Institute, Lomonosov Moscow State University)

Commentators:
-Rinat Sharyapov (The Head of Department, Information Security Institute, Lomonosov Moscow State University
-Keiko Kono (Researcher, National Institute for Defense Studies)
-Yu Koizumi (Special Researcher, Institute for Future Engineering)

Closing Remarks: (17:00 – 17:10)
-Vladimir V. Sokolov (Vice-Director, Information Security Institute, Lomonosov Moscow State University)

Media NHK BS News
TV Asahi News, BS Asahi News Program "Ima Sekai wa"
Booklet of speeches and presentations in English and Japanese

Reception (17:30 – 19:30) Room "Sagami"

Opening Speeches:

Tokai University 75th Anniversary Memorial International Cybersecurity Symposium

December 1, 2017

Yoshihide Suga
(Chief Cabinet Secretary, Government of Japan)

My name is Yoshihide Suga and I am Chief Cabinet Secretary within the Japanese government. I would like to say a few words about this event, Tokai University 75th Anniversary Memorial International Cybersecurity Symposium, cohosted by Tokai University and Moscow State University. As you are all aware, Prime Minister Shinzo Abe and President Vladimir Putin have held 20 summit meetings. Both leaders have a sincere determination to resolve the issue of a peace treaty, and the Japanese prime minister has repeatedly been involved in negotiations with Russia to this end based on a stance of needing to resolve the issue of the four islands prior to concluding a peace treaty. Amid this bilateral relationship, cybersecurity is one area in which it is expected that the two countries will build more cooperative relationships in the future. As the person charged with ultimate responsibility for the government's cybersecurity operations, I welcome the fact that this symposium is being held with the cooperation of both universities. I would also like to sincerely welcome the attendance of David Ellis, Chief Minister, British Embassy, at this symposium, as the United Kingdom, alongside Russia, is another leader in this particular field. The Japanese government is undergoing concentrated investment in policy resources in order to realize "Society 5.0", a society where cyberspace and real space are integrated, and the latest technology is incorporated into all aspects of industry and social life. On the other hand, the cyberspace forming the foundation of Society 5.0 faces the growing threat of malicious cyberattacks. Looking at Japan's government base alone, it was attacked about 7.11 million times last year, or once every 4.4 seconds. Also, this April, we saw many cases around the world where nations were unable to use their systems and data when they came under attack from ransom-type cyberattacks. Given this, securing cybersecurity is an urgent issue. The Cybersecurity Strategy Headquarters, where I serve as Chief, works under the control of the Prime Minister's Office and aims to advance measures relating to cybersecurity. In July of this year, the Cybersecurity Strategy Headquarters compiled an array of measures to accelerate and strengthen Japan's cybersecurity efforts. Today, I would like to introduce you to three points which are earmarked as particularly important.

The first point is the strengthening of security measures for IoT devices. The number and types of IoT devices have been increasing year by year, and it is now expected that in around 2020 the number of IoT devices will hit around the 30 billion mark, and the number of devices that connect to the Internet will far exceed the number of people. It is expected that various data obtained from the various production of IoT devices will be utilized as big data, and AI and the like will use that to create a new wisdom. We believe that Japan must also work with other countries to strengthen security measures for IoT devices.

The second point is to strengthen the sharing of and cooperation relating to security information.

The implementation of cybersecurity measures by users is, of course, the basic of basics, but there is a limit as to how much one person or one entity can do. For this reason, we believe it is important to, after establishing a certain level of rules, such as those relating to confidentiality, advance security measures that share necessary information among those involved in information management quickly and effectively. It is with this point of view in mind that the government wants to build a framework that drives the provision and sharing of useful information in order to promote cybersecurity while working in conjunction with both private businesses and administrative institutions both within Japan and abroad.

The third point is preparations for the Olympic and Paralympic Games Tokyo 2020, which will now be held in less than 1,000 days. The government is currently preparing to build a "Cybersecurity Incident Response Coordination Center" by the end of fiscal year 2019, so that it can respond quickly and accurately to any cyberattack that may occur during the Olympic Games and to ensure smooth operations of the Games. This center is not only necessary for the successful operation of this event, but we will be able to leave all cybersecurity experience and knowledge obtained from operating such a center as a legacy of the Games. We would like to continue our efforts to make Japan into a country that can provide high-quality safety and reliability within cyberspace as well.

Cyberspace is globally connected, making international cooperation extremely important when advancing cybersecurity initiatives and building safe cyberspace.

During today's symposium, I believe that some prominent researchers and professionals from both Japan and Russia will participate in a discussion on "Cybersecurity Dialogue in Global Paradigm Shift".

I think that today's theme is closely related to the three points I just touched on. The government pays close attention to a potential new international framework for the two countries to be established in the wake of the symposium, so as to promote cooperation in the area of cybersecurity further. I look forward to some lively discussion and I also hope that today's content will be fruitful for all involved.

Finally, I sincerely pray for the success of all those in attendance at this symposium and I look forward some great results.

Opening Speeches:

Tokai University Cyber Security Symposium

1 December 2017

David Ellis
(Chief Minister, British Embassy)

Chief Cabinet Secretary Suga, Chancellor Yamada, Ambassador Afanasiev. Thank you very much for the kind invitation to speak here today. It is a pleasure to be here at the Tokai University Club for such a prestigious symposium on cyber security. Especially with such distinguished academics, government representatives and delegates from around the world. I regret that Nigel Inkster was unable to attend for health reasons, but am honoured to be here to represent the UK.

It is particularly good timing to be discussing cyber security issues. Over the last year, we have seen a significant increase in the scale and severity of malicious cyber activity. The global Wannacry ransomware attack in May. Hack and leak operations with En Marche in France. And attacks against the email accounts of UK Members of Parliament.

These are exciting times. The UK is taking a holistic response to these challenges - it requires short and longer term solutions.

Working with allies to respond to cyber-incidents and impose costs on malicious actors. Welcoming and encouraging the implementation of confidence building measures in the ASEAN Regional Forum. And improving the capability of our partners in South East Asia with cyber capacity building programmes.

And of course working with allies is a crucial part of the response. When our Prime Minister visited Japan in the summer, she and Prime Minister Abe issued a joint vision statement, which set the direction for the future of our relationship - taking our partnership to the next level.

The two leaders agreed to strengthen our growing security partnership around the world. This includes defence and foreign policy. But cyber security was central – both countries are publicly committed to reacting to shared threats and deterring threats as they appear.

The two Prime Ministers also agreed to strengthen our economic and business partnerships Cyber security is very important for our economic agenda too. New technology – such as AI, the internet of things, digital services – are crucial engines for growth, and quality of life as this symposium will explore.

Our economies rely on a free, open, and peaceful internet. But to be successful it must be secure, and able to adapt to cyber threats. And unfortunately as I have said those threats are increasing in number and sophistication. The key to tackling Cyber threats effectively is partnership. Between countries, of course. But also between governments and the private sector.

For the UK, the National Cyber Security Centre has been key to our response. The NCSC is the centrepiece of the UK's new Cyber Strategy. Prime Minister Abe visited the NCSC during his trip to London in April, to learn about how it helps the whole of the UK prepare against attacks, and to respond to them when they occur.

The NCSC acts as a single point of contact between government, UK business and academia. It provides advice and support to all parts of UK society, working to strengthen the private sector's capacity to build the skills and capability to take advantage of global cyber opportunities. And it has a key international role in working with other governments to share best practice and respond to threats.

The NCSC was born in part from our experience of hosting the Olympic and Paralympic Games in London in 2012. An exciting time. But also one that produced many cyber threats. Uniting our government security community and the private sector to deliver a safe and successful games, transformed our long term approach to cyber security too.

The eyes of the world will be on Tokyo in 2020, and I am sure we will see the best of Japan – professional, innovative and global. Prime Minister May committed the UK to supporting Japan to help ensure the physical and cybersecurity of the Tokyo Games, building on our London2012 experience. We will continue to work together. Thank you.

Yoshimasa Suenobu

(Director, Strategic Peace and International Affairs Research Institute of Tokai University)

Background and aims of the symposium

My name is Yoshimasa Suenobu and I am the Director of the Strategic Peace and International Affairs Research Institute of Tokai University. I would like to start off by thanking everyone for taking time out of their undoubtedly busy schedules to attend and participate in today's symposium. I realize how valuable time is, so I would just like to briefly talk about the background and aims of today's symposium.

The Strategic Peace and International Affairs Research Institute of Tokai University was established based on the philosophy of Tokai University's founder, Dr. Shigeyoshi Matsumae, and it continues to work based on that philosophy of "human security". Since its establishment, research has predominantly focused on international relations, preventive medicine, and migration and refugee issues within the Asia-Pacific region. This financial year, however, we have started to research global "security frameworks", with the focus on cybersecurity, as this is an urgent issue.

Even during the Cold War, Tokai University and Moscow State University had been involved in academic exchanges. The cohosting of this symposium on cybersecurity, an issue which will have a decisive impact on the future of the world, with such a university in the 75th anniversary of Tokai University's founding is very befitting. This was only achieved with the cooperation of Japanese government and The Sasakawa Peace Foundation, which has a track record in this field, mainly in the United States. Chairman Nobuo Tanaka from The Sasakawa Peace Foundation is also in attendance today and I would like to take this opportunity to express our gratitude for the Foundation's continued support.

We consider the United States, Russia and China as being at the forefront of cybersecurity. Just ever so slightly behind these nations are the United Kingdom, France, Israel and Japan. Based on this recognition, symposium organizers hatched a plan to invite experts from Moscow State University in Russia, a country with which we have been unable to accurately discuss cybersecurity in the past due to the lack of a pipeline to gather information and resulting in the conveying of a small amount of false information. Next year, the Strategic Peace and International Affairs Research Institute of Tokai University plans to provide a forum for discussion on international frameworks. In addition to Russia, we plan to utilize the strong pipelines of The Sasakawa Peace Foundation to have numerous cyber superpowers including the United States, China and Israel, in attendance.

In the first section today, we will be talking about the basic approach and way of thinking on the part of Japan and Russia, including how both nations view and approach the issue of security. There will then be a short coffee break before the second section. This will cover security and the perspectives of both governments, but will also look at the economic sector, especially cybersecurity

within the business sector as this has become a major issue as of late. We have some wonderful commentators participating today, including Ms. Kono from the National Institute for Defense Studies, so I am expecting some lively and frank discussion.

Finally, cyberspace is not a world that we can actually see. In other words, we should realize that fear can exist within, but that hope can also be hidden within. It is my sincerest hope that today's symposium will serve as a starting point for constructive discussion on how to identify where fundamental gaps exist and how we can build international cooperation.

Media

Reports on the symposium were broadcast the same day on NHK News, NHK BS News, TV Asahi ANN News and Abema TV. In Addition, BS Asahi introduced the symposium in a special feature on cybersecurity as part of its "Sunday Scoop" program on January 21, 2018.

Vladislav P. Sherstyuk

(Director, Information Security Institute, Lomonosov Moscow State University, Advisor of the Secretary of the Security Council ofRussian Federation)

Dear organizers of the symposium! Dear participants! Ladies and Gentlemen! Colleagues!

On November 1st this year, Moscow State University's President, Academician Victor Sadovnichy took part in the celebration of the 75th foundation anniversary of Tokai University. This unique educational institution, which has been cooperating with Moscow University since 1973, was founded by Dr. Shigeyoshi Matsumae in 1942.

On behalf of the Moscow State University Institute of Information Security Issues we offer our congratulations to students, post-graduate students, professors, personnel and executives of Tokai University upon this remarkable anniversary! We are grateful to the Rector of the University, Mr. Kiyoshi Yamada, for the invitation to take part in the Symposium on the Modern Trends in International Information Security.

The next year marks 20 years since the term "International Information Security" appeared.

This process was initiated by a special message from the Russian Minister of Foreign Affairs I. Ivanov sent on September 23, 1998 to the UN Secretary-General Kofi Annan.

The 1999 UN General Assembly resolution on "Developments in the field of information and telecommunications in the context of international security" first formulated a "triad of threats" in the field of international information security: the use of information and communication technologies (ICTs) for military, terrorist and criminal purposes.

A discussion on preventing the negative consequences of the ICTs application in the context of international security, disarmament and other areas related to this process continues at the UN General Assembly sessions every year.

The international community notes that at the present stage of development and introduction of information technologies and telecommunications there is a growing danger of using these technologies to violate international peace. At the same time, special attention is drawn to the need of preventing interstate confrontation, which can provoke a new round of the "arms race" in the information field.

In our opinion, one of the most effective ways to address these problems is to strengthen international information security.

A number of international conferences and seminars, including those held under the auspices of the United Nations Institute for Disarmament Research and the International Committee of the Red Cross, were focusing on international information security. Initiated by Russia, at the 56th session of the UN General Assembly on November 29, 2001, a fundamentally important decision was taken to establish an ad hoc group of governmental experts (GGE) to study the problem of international information security. The group was established in 2004. The mandate of the group includes a review of the threats in the field of information security and possible cooperative measures to address them, as well as relevant concepts aimed at strengthening the security of global information and telecommunication systems.

The research efforts of the UN GGE made it possible to focus the attention of all UN member states on the threats to international security and peace caused by the possibility of malicious or hostile use of ICTs by states against territorial integrity and the political independence of other states. The attention of the international community was also drawn to the danger of using ICTs by non-state

entities to prepare or commit terrorist acts, as well as other criminal acts.

As a result of many years of efforts by the GGE, in 2015 a consensus report to the UN Secretary General was adopted, which in many ways can be called a breakthrough. It formulated principles for the responsible behavior of States in the ICT environment, as well as recommendations on confidence-building measures.

The parties agreed on several key things:

First, not to legalize and not to regulate conflicts in cyberspace, but to prevent the use of ICTs for military and political purposes.

Second, to avoid mutual accusations of cyber attacks, as it often happens now, without serious evidence.

Third, ICTs should be used exclusively for peaceful purposes.

Fourth, placing Back door or other implant tools into IT products was recognized as illegal and harmful.

Fifth, the GGE confirmed the sovereign right of states to control ICT infrastructure on their territory and to determine their policy on international information security.

Unfortunately, the group established in 2016 failed to support the momentum and could not reach consensus in preparing the final report, but this should not stop the discussion on key issues of international information security and, moreover, should not be used as an excuse for devaluating the role of the UN and downgrading the discussion to the regional level or even into a bilateral format.

It can be said that the development of ICTs and their use over a wide range of action have not yet made the world safe and more comfortable for people. The danger of the hostile use of ICTs continues to increase with a view to forceful resolution of international disputes over supporting the international terrorist activities, committing cross-border economic fraud, and violating human rights and freedoms. It is becoming a trend of modern international policy to use fake events as an excuse for mounting international tension. Computer attacks are becoming more advanced and sophisticated. The number of attacks on critical governmental and financial facilities and infrastructure does not decrease.

Secretary of the Security Council of the Russian Federation Nikolay Patrushev said that in 2016 the number of cyber attacks on government agencies' websites increased up to 52.5 million cases, while in 2015 there were 14.4 cases. It gives us a threefold increase just in one year. According to the data of the Russian Federal Security Service (FSB), published in January 2017, in recent years the damage from hacker attacks around the world has been estimated from 300 billion to 1 trillion dollars. These losses range from 0.4% to 1.5% of the world's GDP and tend to grow steadily. The risk of hostile use of ICTs by international terrorist organizations, as well as some states, is increasing with the aim of disrupting the working capacity of critical facilities and infrastructure.

Real, virtual and fake events turn the information sphere into phantasmagoria and create significant uncertainties in a person's political life.

The trust between a state, business and the private sector in cyberspace and the information sphere cannot be regarded as a phenomenon independent of the political, economic and social spheres, as well as international life. Confidence will never grow unless we support international cooperation and the discussion of complex problems of international security. We must strive to prevent international conflicts in which both traditional and cyber weapons are used.

The Russian Federation together with the other concerned states conducts significant work on the formation of confidence-building measures, using the site of the Organization for Security and Co-operation in Europe. In 2016, the OSCE Permanent Council decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs. An Informal Working Group to develop CBMs in the field of cyber security was established with the participation of the states concerned.

Through the efforts of the concerned states, including the Russian Federation, the international expert community is beginning to understand the need to comply with international obligations stemming from the sources of international law recognized by the states: general and special international conventions, international custom, general principles of law recognized by civilized peoples, court judgments.

The main features distinguishing the ICT environment from other domains of relations between the sovereign states (like land, sea, air and space) are:

the artificial nature of the ICT environment, being comprised of the combination of telecommunication networks, computer hardware and software and functioning in a global digital code system, operational capacity of which is mostly supported by non-governmental organizations located in different jurisdictions;

the virtual nature of ICT processes, which makes it impossible to directly observe the triggering events of incidents in the ICT environment;

the difficulty to identify the sources of incidents in the ICT environment;

destabilizing consequences of malicious or hostile use of ICTs against critical public infrastructure, as well as terrorist attacks on ICT facilities and ICT-related infrastructure;

the use of ICTs by terrorist organizations to recruit supporters, finance, train, incite and carry out terrorist attacks.

The use of ICTs for interference in the internal affairs of sovereign states should be recognized as a threat to international information security. Russia and several other states have repeatedly stated the need to counter this threat, both at the level of bilateral consultations on information security issues and at the level of the Shanghai Cooperation Organization. The Russian Federation together with other states twice, in 2011 and in 2015, introduced drafts of relevant resolutions to the UN.

Today, in the expert international community one can note discrepancies over the basic principles of the formation of the international information security system. Some of them proceed from the fact that the information space has already become a new theater of military operations and propose to concentrate efforts on regulating the inevitable, in their opinion, military and political conflicts using ICTs. It has been argued that regulatory mechanisms should be based on the unconditional applicability of existing norms of international law, which were created in the pre-digital era. They do not see the need to agree on the establishment of state responsibility areas in the ICT environment, on a procedure for objectifying data on violations of international obligations by states, or on the procedure for investigating international incidents in the ICT environment based on the interaction of national Response Groups for cyber incidents (=Computer Emergency Response Teams, CERTs).

Given that it is virtually impossible to reliably identify the sources of computer attacks, we believe that this approach actually legalizes the possibility of conducting not only information but also military operations against so called "uneasy" states.

Another approach supported by Russian experts is based on preventing the militarization of the information space and non-interference in the internal affairs of other states, and on the unconditional recognition of the digital sovereignty of states. We consider unacceptable the use of unsubstantiated charges of committing computer attacks as an instrument of political pressure.

Despite the above discrepancies in approaches, we believe that we all should concentrate on preventing conflicts in the ICT environment and prohibiting the use of ICT for achieving military objectives, as well as on the progressive development of international law and its adaptation to the specifics of the ICT environment as a new space for international cooperation.

Here are our proposals:

Let us note the primary tasks in the sphere of international information security, on which the international scientific and expert community should be focused:

1. Preparation of the draft Convention on International Information Security in order to formalize the main approaches to the progressive development of international law in relation to the

ICT environment through the adoption of legal rules clarifying the content of international obligations of states in the ICT environment, the procedure for identifying violations of these obligations, singling out subjects that have violated international obligations, as well as procedures for the peaceful settlement of international disputes related to incidents in the ICT environment.

2. Preparation of draft guidelines on the application of principles, norms and rules of responsible behavior of states in the ICT environment.
3. Preparation of the draft Convention on Combating Cyber Crime.
4. Preparation of draft amendments to existing international treaties specifying the content of international obligations in the ICT environment, and, first of all, in the context of preventing international conflicts and the peaceful settlement of international disputes.
5. Preparation of a comprehensive? international agreement on the delineation of the states' areas of responsibility in the ICT environment and the legal securing of these areas (the spatial limits of the sovereignty of states in the ICT environment).
6. Preparation of international agreements on the procedure for investigating international incidents in the ICT environment based on the cooperation between national Centers for Responding to Dangerous Events in this environment, as well as the procedure for attributing responsibility for these incidents to the subjects of international law.
7. Establishment of an international body to arbitrate international disputes on the security of products containing ICT functions, as well as on the use of ICT for interference in the internal affairs of sovereign states.

In our opinion, a research work can be conducted simultaneously in several directions.

First, in the direction of developing bilateral cooperation between the states concerned. This cooperation could be focused on establishing interaction between public authorities in order to: counteract the commission of crimes, the preparation and implementation of terrorist acts; form approaches to the practical development of confidence-building measures appropriate to the level of bilateral relations; apply rules of responsible behavior of states in the ICT environment.

The second area of cooperation may be the development of regional systems for ensuring international information security. Here it is important to develop methods for applying recommendations on confidence-building measures and voluntary rules, principles and norms of responsible behavior of states in the ICT environment, taking into account the international obligations assumed by states within the framework of regional cooperation agreements.

Finally, as a proposal, it would be worthwhile to consider the feasibility of creating, with one of the international organizations or the International Law Commission under the UN General Assembly, a specialized working group for the preparation of proposals for draft international treaties. It would be important for this group to include lawyers, engineers and representatives of law enforcement agencies of the states concerned. The expertise of draft documents prepared by a specialized working group could be carried out by the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security. A compromise on these draft documents could be reached in the format of bilateral and multilateral consultations.

In our opinion, a certain contribution to the solution of the formulated tasks could be made by the Moscow University and Tokai University, including the format of joint research.

This kind of cooperation would promote the international community towards a safer world in the context of the formation of a global information society.

Thank you for your attention.

Moderator:

Ichiyo Ishikawa

(Senior Commentator, Former Chief of Moscow Bureau, NHK)

Sovereign democracy and cybersecurity

This discussion was written in St. Petersburg in the middle of February 2018. The election will, in all likelihood, result in an overwhelming victory to incumbent President Vladimir Putin. However, even at this point as the election is coming into its final days, the question of "who will be the successor" remains unanswered; no one has articulated what it will look like to "travel with Putin" into the post-Putin world. Indeed, the election is defensive in tone, with Mr. Putin running on his track record.

The annual State of the Union Address, which would normally have been given in December of the year preceding an election, had still not taken place by the middle of February. Coming before a president election, the address is essentially a manifesto for the next term and is prepared by a very small number of people closest to the president, under the leadership of Anton Vaino, Chief of Staff of the Presidential Executive Office. But it has yet to be published. One can perhaps glimpse in this the hesitation of the genius populist Putin. It is up to him to somehow balance the objectives of protecting the sovereign state of Russia while also exposing it to global competition.

Of particular interest is what position the President will take on security in cyberspace, where both sovereignty and national borders are ambiguous. If the primary objective is to maintain sovereignty, but policy is too weighted towards security, the country risks losing competitiveness. However, openness to global competition also risks Russia's sovereignty. The question of cybersecurity is a major problem for Putin's approach to maintain "sovereignty" above all else.

On December 1, 2017, the Strategic Peace and International Affairs Research Institute of Tokai University held a Japan-Russia cybersecurity symposium titled "Tokai University 75th Anniversary Memorial International Cyber Security Symposium." In Russia, all aspects of security strategy and doctrine fall under the Security Council. The Information Security Institute of Lomonosov Moscow State University, which has significant impact on the Council's thinking, participated in the symposium as the organizer from the Russian side. From Japan, the government sent people in authoritative positions from the National Center of Incident Readiness and Strategy for Cybersecurity and Ministry of Foreign Affairs, creating an unprecedented event that launched a frank dialogue between the two countries on the field of cybersecurity.

What does a "sovereign state" mean to Russia?

All countries are sovereign states, and respect for sovereignty is at the heart of Russian foreign policy. Even in Syria, where there is a sharp conflict between Russia and the West, Russia justifies the presence of its troops because it was requested to send them by the sovereign state of Syria, and it sees the intervention of the United States and its allies without a request from the Syrian government or a United Nations Security Council resolution, as an illegal act under international law.

However, there is another meaning of the term "sovereign state" in the Russian context. Particularly when we are talking about Russia as a sovereign state, the term takes on a special

meaning. One aspect of sovereignty is decision-making authority. The "security strategy" laid out by Russia in December 2015 defines security to include not only military, political and economic aspects, but also cultural and historical traditions, education and science, and the environment. Using this Russian concept, there are relatively few true sovereign states in the world. Obviously, European countries are not true sovereign states because they have ceded political and economic sovereignty to the EU; likewise Japan, which depends so much on the United States for its defense, may not be a true sovereign state from the Russian perspective. As Russia wants to be a true sovereign state with its own decision-making authority, security in cyberspace therefore poses a major problem for it.

"Bad" Western influences from the borderless Internet could undermine the Russian state, and conversely, Russia could find itself cut off from the Internet infrastructure, which is controlled by the United States. Russia, it would seem, has failed to establish its "sovereignty" in cyberspace. That is also true of Japan and most other countries.

National borders in cyberspace

For Russia, cybersecurity is a question of how to establish sovereignty in cyberspace. Indeed, Russia's biggest objective in cybersecurity is to draw national borders in cyberspace. At the same time, Russia also wants to establish equal rights among the states in cyberspace. Mr. Anatoly Streltsov, Vice Director at the Information Security Institute of Lomonosov Moscow State University and counselor to the Security Council of Russia, proposed at the end of the symposium a draft United Nations convention on "Concepts for the Safe Functioning and Development of the Internet." For Russia, cybersecurity means the establishment of sovereignty in cyberspace. In other words, the highest priority issue is the drawing of national borders, and that can be seen clearly from the Russian proposal: "States shall not use connection to the Internet as a tool to influence other countries," "States shall not restrict the Internet or access to the Internet within the territories of other countries" and "Countries shall recognize the principle of equality in Internet governance and the sovereign rights of states to establish Internet norms for their countries."

That raises the question of what Japan's position is on cybersecurity. "Free, fair and safe cyberspace is a global common medium that enables communication on a global scale and is a foundation for peace and stability in the international community. In particular, Japan believes that recognition of the diverse values in cyberspace, respect for independence, and guarantees that peoples' discussions and corporate behavior will be governed by the rule of law will help to achieve peace, stability, and ultimately, prosperity for the international community" (excerpt from Japan's Cybersecurity Strategy). Japan argues both for respect for existing international laws in cyberspace and for cyberspace as a global common medium. In this symposium, Ms. Kono of the National Institute for Defense Studies raised the question of whether the concept of national borders was valid in cyberspace and noted that the phrase "national borders" appears nowhere in Japan's cybersecurity strategy. Mr. Misumi from the National Center of Incident Readiness and Strategy for Cybersecurity, one of the drafters of Japan's cybersecurity strategy, noted that cyberspace is artificial and is established not by states but by private-sector investment. Investments in cybersecurity need to be recognized as an investment activity that produces value, not as an unavoidable cost to be borne by the private sector. Like the United States, Japan respects the values of freedom and independence, which is a vast difference in thinking from Russia, which argues that national sovereignty should be protected.

It is precisely because of these differences in thinking that it is important to attempt a second track in which experts from Japan and Russia, including government officials, can engage in free discussions of cybersecurity. It is important that Russia be constructively involved in international cybersecurity so that cybersecurity is an area not for conflict, but for cooperation, among states. The cybersecurity dialogue between Tokai University and Lomonosov Moscow State University has a major role to play, and I look forward to seeing it continue.

Presenters:

Ikuo Misumi

(Councillor, Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity, Cabinet Secretariat, Government of Japan)

The importance of cybersecurity initiatives conducted via collaboration among diverse parties

1. Introduction: Background and awareness

With Information and Communication Technology (ICT) becoming increasingly positioned as an essential foundation for economic and social activities, the importance of securing cybersecurity is also increasing. The frequent reporting of cases and incidents involving cybersecurity in the media has led to increased concern about cybersecurity, not only within experts in this field but also among the general public. In Japan, however, many people view cybersecurity as a technical issue. For this reason, few people view cybersecurity initiatives as an issue for their own organization or an issue close to themselves. Many consider cybersecurity initiatives as a cost burden as it is difficult to determine how far measures need to be taken and what kind of measures should be implemented.

This situation seems to resemble discussions surrounding pollution in Japan in the 1960s. Pollution, such as air pollution caused by factories pumping out smoke emissions, became a major social problem. The government established laws and standards aimed at controlling pollution, factories invested in equipment and facilities, and the public learned what to be careful of and how to respond to certain conditions, such as photochemical smog. At the time, measures to deal with pollution were possibly regarded, to a certain degree, as being an unavoidable cost. However, as a result of everyone's efforts, we can see some remarkable results of pollution control, such as the clean air we now have. Today, in many cases, rather than such measures being viewed as a cost burden, they are recognized more positively as an environmentally-friendly approach. In fact, this type of effort is now being looked at as a means to reduce costs by saving energy and, in some cases, this has evolved into profit-making activities for those involved in the environmental business sector.

When thinking about cybersecurity, it can be said that cyberspace is filled to the brim with illegal programs and the like. It is not feasible to think that any one cybersecurity organization can sufficiently respond and deal with cybersecurity incidents as they occur, as they can occur at any time and in any place. It is essential that all parties working on the development of and utilizing ICT join together to strengthen cyberspace together.

In particular, it should be noted that cyberspace is an artificial space predominantly built by private investment. In order to make cyberspace safer, it is important for the private sector to also invest further in cybersecurity measures. To this end, it is necessary to promote the recognition that investment in cybersecurity is not an unavoidable cost burden, but rather a positive value-generating investment. Given this background, this paper emphasizes the importance of measures aimed at securing safety within cyberspace from the economic perspective and, with that in mind, introduces the latest approach to cybersecurity within Japan, including concrete examples.

2. Japan's cybersecurity strategy

Cybersecurity-related measures in Japan are implemented in accordance with its Cybersecurity Strategy approved by Cabinet in September 2015 (2015 Strategy). This strategy defines cyberspace as "an artificial space, a frontier that can produce infinite value". Just as public key cryptography was essential for the development of e-commerce, ICT has become a foundation for creating added value within business. Defining cyberspace in this way plays a huge role when trying to encourage private investment in cybersecurity.

The three main pillars within this strategy are measures related to the sustainable development of the economy and society, measures related to the safety and security of people and society, and measures relating to the safety and security of Japan and the rest of the world. The strategy is also

organized into cross-disciplinary and fundamental fields, such as research and development and human resources development.

In more concrete terms, as a measure related to the sustainable development of the economy and society, the first priority was to promote the inclusion of a cybersecurity perspective in corporate business strategies. For example, today, the introduction of Internet of Things (IoT) devices, such as security cameras which utilize Internet technology, has increased exponentially. Customers demand high quality and a high level of safety from such devices. In this IoT era, it is chips and software that makes something functional. As such, in order to respond to the demands of customers, the manufacturing industry can gain a competitive edge by providing cybersecurity as a quality and cybersecurity that guarantees the safety of products and services. Accordingly, it is important to promote a mind-shift within management involved in the manufacturing sector whereby they become aware that a business strategy to secure cybersecurity as a quality will create added value. The relevant government ministries and agencies are currently working together to promote related measures, such as the development of guidelines for management.

In order to conduct economic and social activities in cyberspace, cyberspace must be safe and reliable. This is why the second pillar of the strategy covers cybersecurity measures to protect the public from cybercrime and to protect the safety and stability of services delivered by the government and key infrastructure operators, such as electricity and telecommunications operators. As the Internet is global, the third pillar of the strategy is to promote international cooperation. Also, cybersecurity measures within organizations involved in security, such as the Self-Defense Forces, are also to be strengthened in order to maintain mission security. In addition, Japan is steadily developing systems from the perspective of securing cybersecurity at the Olympic and Paralympic Games Tokyo 2020.

3. Interim review of strategy

The period covered in the 2015 Strategy was three years, and the government implemented an interim review of the strategy approximately two years in July 2017.

The reason they did this was because the situation surrounding cybersecurity had somewhat changed since the establishment of the strategy. For example, in the fall of 2016 there was a large-scale Distributed Denial of Service (DDoS) attack that caused disruption for numerous businesses, such as twitter, and there was also the ransom-type attack in May 2017 where, within a short period of time, tens of thousands of computers in more than 150 countries were infected by a malicious program. These types of incidents, still fresh in our minds, impede economic development by hindering smooth corporate activities utilizing cyberspace. For this reason, and based on the changes that had occurred, the government decided to conduct an interim review to clarify what measures should be given priority in the last year of the 2015 Strategy.

The basic idea here, just as it was when considering anti-pollution measures, is that all concerned parties should work on measures, including preventative measures. This is very similar to a public health approach in that everyone works together to make cyberspace clean.

Based on this concept of cyber hygiene, it was decided that the following should be given priority: (1) bot eradication measures, (2) information cooperation network, and (3) accelerating preparations for Tokyo 2020.

In addition, in order to promote the development of the economy and society via cybersecurity, efforts to establish an international standard aimed at safe IoT systems are being rolled out and measures aimed at promoting security within universities and so on so as to protect advanced technology currently being developed and strengthening international collaboration are included.

Below, I will provide a brief introduction of the three measures given priority.

First of all, there is bot eradication. Let us consider why bots are a threat. A bot can remotely control a computer or an IoT device infected by the attacker as if it were a robot. When a large number of bots are networked an attacker can carry out cyberattacks on a large-scale. This is not limited to DDoS attacks but is a hotbed for a range of attacks and crimes. In particular, given the growing number of vulnerable IoT devices, early efforts are required to clean cyberspace.

For this reason, the Ministry of Internal Affairs and Communication, in particular, utilizes a cyberattack observation network and search methods to detect IoT devices that are vulnerable within networks, to conduct surveys on IoT devices connected to the Internet, particularly those IoT devices that are highly likely to directly impact people's lives and social living. When they identify an IoT

device which is vulnerable to a cyberattack, the owner and so on are alerted, or, when required, technical information on a device's vulnerability is provided to the manufacturer. A law was also revised for this purpose.

Next is the formation of an information cooperation network. In order to prevent the spread of damage once the threat of a cyberattack or the like has been recognized, threat information, vulnerability information, countermeasure information and so forth needs to be shared among concerned parties, including technical experts, as soon as possible. The concerned parties should then work together on concrete protection measures. However, organizations that have been subjected to a cyberattack are often reluctant to share information as they fear that this will tarnish their reputation or have a detrimental impact on them. This makes it difficult for technical experts within such an organization to smoothly share information with other technical experts in another organizations.

In order to overcome such restraints, a community of cybersecurity experts should be formed, and once becoming a member all members must agree to be bound by a duty of confidentiality. In order to do this, the Cabinet approved revisions to the Basic Act on Cybersecurity and I am hoping that an even deeper level of discussion on cybersecurity will ensue within the Diet.

Third is the acceleration of preparations for Tokyo 2020. Security is essential in order to achieve a high-quality and safe Olympic and Paralympic Games. Given the penetration of ICT, cybersecurity is an important aspect of overall security. In particular, in order for the Games to be conducted smoothly, securing essential services such as electricity, broadcasting and so forth is necessary. Physical countermeasures, such as a backup power supply, are required in order to secure an uninterrupted supply of these services. In the same way, countermeasures for cybersecurity incidents, which also could potentially disrupt such services, are considered important.

For this reason, companies that provide such essential services must, in accordance with a manual produced by the government, conduct cybersecurity risk management from the perspective of being able to maintain a supply of its service. A total of six cycles of these measures, including risk assessment, will be carried out leading up to Tokyo 2020. Two cycles have already been completed. In addition, as it can be expected that risk management of individual operators would be optimized for their own business and circumstances, the government conducts cross-disciplinary and overall risk assessment, including the assessment of measures employed by business operators within the same field.

Even if protection is in place in advance, the ability to respond appropriately when an event occurs is essential. As such, the Cybersecurity Incident Response Coordination Center, which will coordinate cybersecurity incidents among concerned parties and promote countermeasures during the Games, will be established by the end of fiscal year 2018. We will also be working closely with organizations providing physical security as we also need to align cybersecurity with real-world services and safety measures.

4. Conclusion: Discussion aimed at developing the next-generation cybersecurity strategy

The strategy decided on in 2015 only covers the period up to summer 2018. As such, the government is currently working on a new cybersecurity strategy. The underlying basic philosophy, described above, within the 2015 Strategy and the Interim Review will remain unchanged. One particular point that is being emphasized is cooperation and collaboration. In other words, for the services and operations provided by each party to be fulfilled, the many diverse parties involved in cyber-related issues should pool their efforts and work together based on risk.

In order to steadily and soundly achieve these initiatives, it is important to enhance the cybersecurity capabilities of all parties involved. In general, the focus is on the identification and training of human resources with advanced technology when talking about human resources for cybersecurity. However, this is not enough. With ICT becoming an increasingly important foundation for the economy and society, along with a mind-shift within organizational management, it is a matter of urgency for Japan to nurture and grow a layer of strategic management who can create management strategies from the perspective of ICT and cybersecurity and can lead cyber professionals while also being involved in risk management themselves. It is important for us to deepen discussions on our next cybersecurity strategy, to implement that strategy, and to contribute to the realization and maintenance of safe cyberspace in which diverse individuals can actively participate.

Presenters:

Anatoly Streltsov

(Vice Director, Information Security Institute, Lomonosov Moscow State University)

Main Challenges of International Information Security Legal Groundwork

Among most important challenges of international information security legal groundwork, there is the problem of applying the international law to relations arising in connection with malicious use of information communication technologies (ICTs) endangering international peace and security. In reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security, it was noted that successful counteraction to this threat required joint efforts of UN member-countries and, in particular, elaboration of a common understanding in respect of application of appropriate norms of the international law, and also norms, rules and principles of responsible behavior of states resulting from the foregoing norms.

1. In spite of the fact that the problem of application of the international law to international relations in the ICT environment is still unresolved, one can hardly assume that there is an approach to its solution that would not be based on the international law norms and principles.

Soundness of this position seems to be determined, firstly, by the following.

Firstly, creation of a new sector of the international law that foeuses on regulation of international relations as regards malicious use of ICTs, in spite of existence of such assumptions, seems unfeasible and inexpedient. It is unfeasible because contemporary international relations are very dynamic, besides, they are considerably impaired by distrust accumulated between permanent members of the UN Security Council and it seems rather difficult to reach consensus on such complex matter in this situation. It is inexpedient because it can be reasonably assumed that in any case new norms and principles will be based on existent norms and principles.

Secondly, the current international law norms and principles have been proven by time and reflect a certain consensus of positions of UN member-states as regards the mechanisms of regulation of international relations in the field of international security. States have accumulated considerable experience of application of the international law norms and principles in discussing specific problems.

Thirdly, nothing in the current norms and principles prevents their application by states for counteraction to security threats instigated by malicious use of ICTs. At the same time, in the absence of special international legal regulation of relations related to ICT environment, there exists a possibility of erroneous interpretation of events taking place in ICT environment. The possible consequences of such erroneous interpretation would be higher risk of occurrence of international conflicts and occurrence of real threats to the international peace and security.

Based on the afore-stated, it seems important to study the challenges of practical application of the international law for counteraction to malicious use of ICTs, so it will not create new threats to peace.

An important step towards reduction of the risk of such development of events is adoption by the UN Group of Governmental Experts of proposals concerning the norms, rules and principles of responsible behavior of states in ICT environment and confidence-building measures. These proposals are aimed at preventing international conflicts related to ICT environment. To study the methods of implementation of the norms, rules and principles of responsible behavior of states in ICT environment, based on discussions at the Munich Security Conference (February 2017), The Global Commission on the Stability of Cyberspace has been established.

It seems that the next stage of investigation of the ways to enable application of the international

law to the new field of international relations will inevitably include the norms and principles of the international material law and the international procedural law determining the rights and obligations of states in the process of fulfillment of material norms.

2. There are grounds to believe that the norms, rules and principles of responsible behavior of states prepared by the next UN Group of Governmental Experts will be finalized as a regulatory legal act and will be supported by UN member-countries. In such case, ICT environment will be an object of the international law and assessment of ICT environment from this point of view will draw attention.

From the technical point of view, ICT environment may be defined as a totality of objects of processing, storage, transmission, distribution, and representation of information, which exist in the space of the global system of digital addresses that are not connected with location of objects on a physical territory and that interact based on a single system of protocols.

Based on this, ICT environment is not a component of the territory of a state, which includes ground, air and water. This environment has an artificial origin and exists thanks to activities of interested persons. From this point of view, ICT environment may be defined as a legal fiction consisting in that this environment is regarded as a component of the territory of a state. This allows extending the notion of 'sovereignty' to ICT environment.

Among the peculiarities of public relations connected with ICT environment, there are, first of all, those that the objects of relations in this environment (information, information systems, ICTs, information processing processes), and, respectively, legal facts conditioning occurrence, modification and cessation of legal relations in respect of objects of ICT environment same as subjects of the relations under discussion have a virtual nature, i.e. they are invisible (indefinite). In this situation, for legal regulation of relations on the basis of sovereignty of a state, it seems important to apply methods of objectivation of legally significant events and processes of ICT environment and attribution of subjects of relations (attribution of responsibility).

ICT environment as an object of international relations can be characterized by inclusion into the global cyberspace and security of its use. In certain circumstances, these characteristics can be considered as aspects of territorial integrity and political independence of a state. Violation of inclusion of the national segment of ICT environment into the global ICT environment, same as violation of security of its use in contemporary society can lead to disturbed functioning of all spheres of public life.

3. Application of term 'sovereignty' to ICT environment gives rise to other problems as well. Here are some of them.

The absence of spatial limitations of sovereignty in ICT environment. This does not allow determining where the sovereignty of one state ends and the sovereignty of another state begins. This issue is particularly important, for example, in determining the borders of an armed conflict engaging national segments of ICT environment when measures are implemented to maintain guarantees of fulfillment of international obligations on a sovereign territory and, in particular, in the national segment of ICT environment, specifically, by means of establishing certain legal regime with this national segment.

The absence of states that assumed international obligations of ensuring stable and secure functioning of the system of distribution and ensuring functioning of the global system of digital addresses and domain names. This is partially caused by imposition of respective functions on non-profit organizations, which are under the USA jurisdiction: Internet Society – ISOC; World Wide Web Consortium – W3C; Internet Corporation for assigned names and Number – ICANN; Internet assigned number Authority – IANA, which do not possess necessary international legal capacity, actual and delictual dispositive capacity.

The absence of universal international acts about international cooperation in the field of ensuring legal guarantees of respect of human rights and rights of citizens abroad of a national territory (privacy, the right of use of the creative activity results). As is known, respect of these rights is the obligation of states, but if information for technical reasons leaves the national territory, fulfillment of this international obligation becomes physically impossible.

The absence of a universal international legal act on the matters of cooperation of states in the field of counteraction to computer crime. It is known that a considerable part of such crimes has

a transboundary nature and their investigation requires usage of information located on objects of national segments of the ICT environment of other states. The existent methods of addressing this issue are insufficiently effective, yet. From this point of view, one can understand the developers of the Budapest Convention on Cybercrime who tried to overcome this inconvenience. It is known that the Russian Federation has not joined this convention. It seems that an obstacle thereto was, specifically, absence of confidence in that the subject of computer crime investigations, while penetrating into the national segment of ICT environment, will be limited to resolving the tasks of investigation and will not make use of this circumstance for other purposes undesirable in terms of national security.

4. In conclusion, proposals on progressive development of information security legal.

It seems that this objective can be achieved through drafting and adoption of necessary addenda and clarifications to the existent sources of international law.

Analysis has shown that all provisions of the UN Charter can be applied to relations in ICT environment. At the same time, it seems important, in addition to this document, to fix clarification of existent norms as applied to use of ICT as a 'force' and means of carrying out an 'armed attack' (correspondingly, article 2(4) and article 51 of the UN Charter). It is worth noting that ICT is not a weapon by definition, but can impart weapon properties to some devices and mechanisms of non-military purpose. So, these devices and mechanisms can be used for execution of an armed attack in the meaning of article 51 of the UN Charter. A test case of such interpretation of an 'armed attack' was created by resolutions of the UN Security Council (2001) based on the results of discussion of the tragic events in the USA on September 11th, 2001. That attack was implemented using civil planes, which are knowingly not a weapon.

Same conclusions can be drawn from analysis of the 1970 Declaration of the Principles of International Law. Provisions of this document do not create obstacles for their application in regulation of international relations in ICT environment either. At the same time, in view of the new sphere of international life possessing a number of specific features, they have to be complemented. In particular, this addendum could fix wordings of some provisions of the Declaration as applied to ICT environment. For example, clarify the notion of 'territorial integrity', 'political independence', 'sovereign equality', and some other.

The principles and norms of the armed conflict law and international humanitarian law fixed in the Hague and Geneva Conventions do not preclude their application to actions wherein ICTs are used as means of 'force' impact on the enemy, too. However, they seem to need clarification. In particular, it would be expedient to determine legal mechanisms of:

demarcation of national segments of ICT environment, which are within the armed conflict zone, from national segments of ICT environment of neutral states;

identification of civil and military objects in ICT environment, without which it is impossible to enforce restrictions imposed by the international humanitarian law on hostilities;

conduct of international investigations for signs of violations of international humanitarian law restrictions by one of warring sides, which authorized bodies must perform, objectivation of facts of unlawful use of ICTs and attribution of persons guilty of such use of technologies.

To minimize the risks of erroneous assessment of a situation by the UN Security Council, such as detection of mass destruction weapons in Iraq (2003), also to identify subjects carrying out unlawful use of ICT as a means of force impact, it would be useful to consider the possibility of creating a system of objectivation of legally significant events and processes in ICT environment and attribution of persons which are subjects of respective legal relations.

The suggested approach allows wording a program for progressive development of the international law in the direction of its adaptation to ICT environment and developing roadmaps of such program implementation on the basis of elaboration of the law development priorities.

The first measure of such program could be preparation of a Guideline for application of the norms, rules and principles of responsible behavior of states in ICT environment. A roadmap of implementation of this measure could enable creation of conditions for coordination of the efforts of UN member-countries towards prevention of international conflicts in ICT environment and concentrate the potential of political experts, lawyers and technical regulation specialists on the most priority directions of studies.

Presenters:

Takuo Nakajima

(Chief, Information Education Center, Tokai University)

Cybersecurity in a Global Paradigm Shift

1. Introduction

When the internet was in its infancy in the 1980s, cyberattacks tended to be committed simply for amusement rather than for the benefit of the perpetrator. Cyberattacks in recent years, however, increasingly have changed their target from individuals to organizations or nations, and organizations are being created for cybersecurity at the national level. The background of these changes is that the internet has become an important technology affecting the politics and economics of the entire world. We have arrived at an age of paradigm shift in which new concepts in the global age go beyond existing concepts. Recent cyberattacks have changed their targets to nations or companies for economic and political gains, elevating this to a major political issue. In this report, we will discuss the fundamental factors as to why cyberattacks continue to exist and introduce/propose methods to detect these attacks.

2. Paradigm Shift

The definition of a paradigm shift is a dynamic change of conventional assumptions and values. We are currently amidst a paradigm shift due to the seamless connection of information previously separated by nation, as well as the personal transmission of information to global society that was previously propagated only by organizations. The "Arab Spring" democratization movement in the Arab region emerged in 2010 largely by the quick propagation of information using the internet. Information control was conventionally one security governance measure, but the internet has brought a major paradigm shift. Information transmission over the internet and cyberattacks with political aims are increasing yearly and have broadened their economic and social influences.

3. Cybersecurity

Cyberattacks had targeted individuals in the past, but companies and nations are now preyed upon for economic and political effect. In particular, national infrastructures, such as water management facilities and power plant facilities, including nuclear plant facilities, are being targeted. In 2015, 430 million new unique malware were found, and in May 2017, a ransomware called WannaCry spread to more than 150 countries and infected over 230,000 computers. The purpose has shifted to gaining political predominance and economic profit, and this may eventually lead to terrorism. As we enter the IoT (Internet of Things) era where various electric devices will connect to the internet, security measures for these devices become necessary.

3.1 Cause of Cyberattacks

One of the causes of cyberattacks is said to be the vulnerability of software and networks. On the other hand, these attacks are often successful because of human vulnerabilities such as trusting without authentication. For example, people tend to insert USB memory sticks to the computer without authentication or open attached files without confirming who sent it. Because internet protocol was originally designed and used in a closed community, it had various functions for mutual connection, but there may not have been adequate thought given to security. E-mail data is not encrypted as it flows through the internet today, meaning it is possible to monitor the e-mail of a

particular person.

A typical method of attack is to spoof the source IP address. Data flowing through the internet are called IP packets, and the control data that indicate their direction flow are stored in the packet header. The source IP address, one of these control data stored in the header could be forged, just like with the postal system. Two-way communication isn't possible, but this type of attack can harass the recipient. As a large volume of packets with forged source IP deluge the server, that server is forced to interrupt service, which is why these attacks are called DoS (Denial of Service). When the attack is carried out by distributed hosts called network bots, this is called DDoS (Distributed DoS). There is a technology/organization called the Onion Router (Tor). This technology controls the flow of packets and by doing so it can make it difficult to trace back to the origin of the packets with forged IP by pushing out these packets from the network. Abusing this technology makes it possible to control data transfer routes across nations; it thereby becomes difficult to identify attackers.

3.2 Targets of Cyberattacks

The target of cyberattacks used to be individuals, but as objectives become political and economic, this has changed to the information management systems of local infrastructures. Accordingly, the security management function of the SCADA (Supervisory Control and Data Acquisition) systems that manage the information of these infrastructures is being enhanced. The targets of cyberattacks today are broad—not only water and gas supply systems, but also railway signal management systems, car assembly factories and even nuclear power plant systems. There is a need to consider defense methods for these distinctive attacks on infrastructure systems.

3.3 Security and Privacy

Security enhancement and privacy protection have a trade-off relationship. In the US, it has surfaced that the National Security Agency has been conducting PRISM (a communication surveillance program) with the support of companies including Google, Yahoo!, Facebook, Apple, AOL, Skype, and YouTube in monitoring private messages. On the other hand, social media is triggering individuals to actively post personal information on the internet. Many people are unaware that locations of photos posted on social media can be identified using GPS functions. Inadvertent leaking of personal information like this can lead to crimes, so there is need to spread accurate knowledge about these services.

3.4 Classification of Cyberattacks

Attackers collect information by scanning the target organization server for vulnerabilities. Different attacking methods exist depending on server type, such as web server, database server, and so forth. As system managers gain security knowledge, the number of direct server attacks have not increased. On the other hand, targeted attacks are more frequent in recent years. A common scenario is to attach a malware file to an e-mail that will launch when the user opens it. If the filename extension of the malware is something recognizable like .pdf or .zip, the user will sometimes carelessly click and launch it without reading the e-mail. Malware files these days are obfuscated and difficult for security systems to detect and analyze its behavior, so it's crucial to raise awareness among users for security as well.

4. Detection Methods of Attacks

4.1 Detection Methods of Cyberattacks

The detection methods for cyberattacks are basically the same as methods in the data science field. Classification methods are used to classify as benign or malware data. Variation indicators such as entropy compare the value of benign and malware data by analyzing with several parameters. This can be handled stochastically by employing class probability estimation or by stochastically calculating the score of elements in each class. With the regression method, we can estimate the values to discern malware data. These data mining methods can be applied as detection methods of

cyberattacks.

4.2 Proposed Detection Methods

We have researched and proposed detection methods of cyberattacks on networks. We especially focused on DDoS/DoS attacks, and these detection methods can be applied to attacks that alter computer behavior, for example being infected by malware and then downloading the malware itself from C&C servers.

Firstly, we proposed a detection method using entropy based on the source IP address of all packets flowing to a specific site. Variation indicators of the packet source IP address are based on the assumption that organizations hold a unique entropy value. When a DoS attack occurs, there will be a higher frequency of packets with a certain source IP address, so the entropy value will decrease compared to the normal condition value. On the other hand, the entropy value will increase under DDoS attacks compared to the normal condition. This method is effective not only for DoS/DDoS attacks, but also for detecting if the computer is behaving differently than usual. Secondly, we have proposed a detection method using Pearson's chi-square value. In this algorithm, each sample data is expected to be classified into bins with the frequency order under the same variable interval. We examined whether the actual values are equally classified or not to detect if the site is under attack. Finally, we have also proposed and evaluated a malware detection method for pdf files using the one-class SVM (Support Vector Machine) [1].

5. Conclusion

The internet plays a role in triggering new social conditions of the paradigm shift; we discussed its pros and cons in this report and indicated how adequate maintenance of security is important in this environment.

Reference

[1] Mai Iwamoto, Shunsuke Oshima and Takuo Nakashima, A Malware Detection Method based on OC-SVM Focusing on Features of PDF Files, ICIC Express Letters - An International Journal of Research and Surveys, Vol.11, No.11, pp.1611-1618, Nov. 2017.

Presenters:

Pavel Karasev

(Information Security Institute, Lomonosov Moscow StateUniversity)

IcTs as Driver of Global Paradigm Shift:
Social, Cultural, Political, and Economic-Technological Trends

According to the recent statistics, at the turn of 2017, a groundbreaking event took place – the next milestone was achieved and now more than half of the Earth's population (3, 9 billion) is already using the global Internet. The number of companies underlying the digital economy increases. National governments progressively use ICTs in their activities and transform the traditional state mechanisms (taxation, regulation and licensing, etc.), develop and implement E-government projects. The active use and implementation of ICTs in all areas of human life also creates a dangerous dependence on uninterrupted and proper operation of information and communication systems. Completely new threats emerge which are based on the use of ICTs' inherent vulnerabilities.

ICT have been underlying the gradual paradigm shift in the social, cultural, economic and politico-military areas during the recent 30 years. It mainly involves such processes as exploitation of the information space, creation of special-purpose ICT tools to exercise the national interests, emergence and development of the Sixth Wave of Innovation and Industry 4.0. The paradigm shift in each of the above areas resulted, on the one hand, in new opportunities for growth and social, cultural, political and economic development, and, on the other hand, in transformational threats.

At the current stage of human development, information became a strategic development resource due to active introduction and use of ICTs giving rise to a new type of society and economy. Japan was the first country where the idea of "information society" actually appeared. The works of Yujiro Hayashi, a professor of the Tokyo Institute of Technology who aimed to create a theory of social and economic development of Japan, can be highlighted here. As you know, the information society is essentially characterized by introduction of information technologies into all spheres of life, increased role of information, knowledge and information technologies in social activities. This requires creation of the global information environment ensuring the efficient communication among individuals, access to world-wide information resources, satisfaction of demand for information products and services.

The rise and development of the digital society is the very shift of the social and cultural paradigm. The way we perceive information, our communication culture, range of interests and circle of acquaintances have changed. Up to date, Facebook, a social media, has more than 2 billion people joined together on its servers. Your "friends" can include a person whom you have never seen before and with whom you only belong to the same affinity group. But who or what does hide behind a social network account which became a reflection of identity, a kind of ID in the information environment? So, we approach the duality we have noted above. Indeed, ICTs provide people with tremendous opportunities to intercommunicate, share their opinion and information. However, people are already unable to make critical assessment of all the information they face. This entails a threat of malicious information attacks that may pursue criminal, terrorist or political goals.

The other area of the paradigm shift is the foreign policy of states. ICTs contributed to the role

of information environment as a new sphere of confrontation. Thus, the cyberspace has already been recognized to be a new scene of operations both at the national level and among organizations. The increasing number of states develops ICT tools to use them for politico-military purposes – according to some reports, the club of "cyber powers" already involves over 60 countries and yet more are waiting to join it. There is a growing threat of impacting the mass consciousness by ICTs to destabilize the public order or disseminate destructive ideas. In practice, the proliferation of cyber weapons is now an uncontrolled process, which has been developing off the existing system of international security. The multipolarization of the world, which in itself is a paradigm shift, intensifies the process since the states, government-type associations and non-governmental actors see ICT tools as a way to compensate the lack of their power in other spheres. For years, Russia has proposed draft treaties to limit or prohibit the development and use of cyber weapons, in other words, advocated prevention of conflicts instead of their legalization and regulation. In fact – the very issue of attribution of cyber attacks still remaining open – a guilty party may be "appointed" by political considerations, and it might not only incur sanctions but also have force used against it. Adoption by the UN Group of Governmental Experts of the Norms, Rules and Principles of Responsible Behavior of States is an important step in the right direction. The next step should be development by the scientific community and experts of certain recommendations how to apply these norms, rules and principles in the ICT sphere.

The most developed countries of the world are already facing the forth industrial revolution and convergence of nanotechnology, biotechnology, information technology, and cognitive science (NBIC) in the economic and technological area. The transition to the Sixth Wave of Innovation and development of the information sector entail changes in the global economic structure, the market becomes more widespread, dynamic and competitive, variety of new types of business emerge, for example, E-commerce. According to some reports, Internet sales in 2018 will approach USD 3 trillion. ICTs form the basis of such new technologies and phenomena as Big Data processing, quantum computing, augmented and virtual realty, blockchain. We are only beginning to boost these innovations and often overlook the related risks and threats.

It is fair to say that we lag considerably behind in the rapid development and implementation of the technologies. Quoting Martin Luther King, "Our scientific power has outrun our spiritual power. We have guided missiles and misguided men." We lack something more important – deep scientific apprehension and understanding of the ongoing processes and projection of their effects. How can a person and the society protect themselves against fake news, political manipulations or impact of terrorist or extremist ideology? How to counteract threats to strategic stability and contribute to equitable strategic partnership in the global information environment? How to ensure the sustainable economic growth and development without sacrificing the security?

One of the most elaborate responses to these questions is creation of a system of international information security, including foundation of new, or broadening of powers of existing, international and national institutes aimed to regulate the activities of different entities of the global information environment. The duty of the university corporation in this system is to elaborate and provide to the mankind responses to both current and future threats. However, this task may not be effectively realized without concerted efforts of scientific teams from different states.

Commentators:

Rinat Sharyapov

(The Head of Department, Information Security Institute, Lomonosov Moscow State University)

Commentary: About some consequences of the mass adoption of the Internet of Things

Good day, dear colleagues!

I would like to thank the organizers of this meeting for the opportunity to make a short comment.

Colleagues, we've all heard numerous interesting and informative speeches on topical issues of International Information Security. I would like to say a few words about some social and humanitarian consequences of the mass adoption of the Internet of Things.

According to Cisco, *the Internet of Things means any devices that can connect to the Internet*[1]. According to Gartner, 8.4 billion devices are expected to be connected to the Internet by 2017[2]. Cisco forecasts that up to 50 bln connected devices will operate by 2020, which means a critical mass in fulfilling the potential of the Internet of Things[3].

The use of the Internet of things technology has a huge potential for developing economics and improving the quality of life. But at the same time, the mass adoption of this technology has significant negative consequences for an individual, society and country.

The leading states of the world and international organizations are consciously concerned about possible negative consequences, new challenges and threats that the Internet of Things technology can bring.

For Japan, a country with a high information and communication technology (ICT) index – 8.43 points (it ranks 10th in the world, according to ICT Development Index (IDI-2017) produced by the International Telecommunication Union (ITU))[4] ensuring cyber security in the conditions of super-stormy development of the Internet of Things is a strategic task in the sphere of national security.

Thus, in August 2016 the National Center of Incident Readiness and Strategy for Cyber Security at the Government of Japan (NISC)[5] prepared the document "General Framework for Secured IoT Systems" containing the main elements of the policy for ensuring the safe functioning of the Internet of Things[6].

In November 2016, the US Department of Homeland Security prepared a document "Strategic principles for securing the Internet of Things (IoT), Version 1.0)"[7], which contains specific recommendations that emerged from the professional discussions.

In the Russian Federation, in accordance with the Digital Economy Program approved by the Government of the Russian Federation on July 28, 2017, work is already underway to revise certain standards and technical regulations from the standpoints, which among others include the need to ensure the information security of the Internet of Things.

Dear colleagues!

Let's ask ourselves: is an individual ready to accept a situation where dozens of technical devices having an access to the global network and working independently with the Internet would be present and act in his/her personal space? Are the manufacturers of technologies and devices of the Internet of Things ready to assume social responsibility for possible social and humanitarian consequences? Apparently not yet!

First, all device manufacturers declare that everything is for the benefit of people, but we are not

aware of each function imbedded in the device.

Striking examples of negative social consequences are precedents in the USA, Germany, Norway, when the so-called "smart" toys with undeclared access to the global network violated the privacy rights, which entailed legal consequences.

The US Federal Bureau of Investigation (FBI) requests parents to check the "smart" toys of their children. According to the FBI, these toys with Internet access, equipped with video cameras and microphones, which record and recognize speech of its owner, simulating a "live" communication, can pose a serious threat for personal safety.

In the current year, an American company "Spiral Toys" that produces "smart" soft toys left more than 800 thousand customer conversation recordings totally exposed online for anyone to listen.

At the same time, in Germany the Federal Network Agency (Bundesnetzagentur) banned the sale of "smart" dolls "My Friend Cayla", calling the toy a spy device [8].

This kind of use of "smart" devices expressly violates the provisions of UN General Assembly Resolution "The right to privacy in the digital age" (A/RES/71/199) of 19 December 2016.

Secondly, the devices connected to the Internet of Things may be hacked from the outside and, with a certain degree of probability, they will not operate for the benefit of individual consumers, groups and societies, but to harm them.

As you all know, the world community cannot cope with cybercrime. And these criminals and criminal groups operating in cyberspace will seize enthusiastically on the new technical capabilities that can be provided by millions of devices connected by the technologies of the Internet of Things, which in turn can cause serious social consequences.

For example, *according to the Japanese press (National Institute of Information and Communications Technology of Japan), 128.1 billion cyber attacks against networks in Japan were registered in 2016, which is more than twice as high as in 2015. In this case, more than 50% of attacks identified last year were launched against targeted surveillance cameras connected to the Internet, home wireless routers and other devices with Internet access; the number of such attacks increased by about 26 percent compared to 2015* [9].

Thirdly, although these technical devices are not full-fledged computer devices and they have limited computation capacities, but, having access to the Internet, they can be used to launch DDos-attacks. This phenomenon was called Botnet of Things.

The most famous example: the massive DDoS attack was launched against the Dyn's Managed DNS infrastructure using the Mirai botnet in October 2016: about 100,000 infected IoT-devices were involved in the attack. A month later, more than 900,000 customers of German ISP Deutsche Telekom (DT) were knocked offline after their Internet routers got infected by a new variant of a computer worm known as Mirai.

Dear colleagues,

Let's ask one more question: is the state ready to ensure information security of its citizens in the context of mass adoption of the Internet of Things (IoT)? The task is super difficult!

Here it is necessary to recall the importance of implementing the provisions of another UN General Assembly Resolution "Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures" adopted on 21 December 2009 (A/RES/64/211).

According to the Trustlook survey (September 2017) [10], *the level of online users' Internet of Things threat awareness is relatively low against the backdrop of the growing number of cyber threats in this field.*

The survey showed that more than a third (35%) of owners of device from the "Internet of Things" do not change the default password, which makes these devices vulnerable to cyber

attacks. In addition, 54% of users do not install any third-party software to protect devices from cybercriminals.

While the use of devices increases, it also increases the risks associated with them. According to experts, the share of cyber attacks against IoT-devices will account for 25% by 2020.

It's sad, but, using "smart" devices, one can have a destructive impact on the operation of any element of critical infrastructure not only for criminal, but also for terrorist and even military purposes. [11]

Dear colleagues!

One of the simplest measures to be taken to protect yourself against risks is compliance with the basics of the information security culture. The necessity to develop, implement and apply information security culture in all cases of interaction with ICT technologies, including the areas of the Internet of Things is the most important tasks.

Our symposium resulted from the long-term and successful cooperation between the Moscow University and Tokai University, two authoritative scientific and educational universities, the main objective of both is the development and training. And here I want to draw your attention to the conceptual article of Moscow University's President, Academician Victor Sadovnichy "How to protect an individual from infogenic risks and threats?" written in 2013 (translated into Japanese as well), which confirms that duty of the ***"scientific and educational corporation is to develop and implement a system of knowledge, skills and norms of global information security culture"***. According to the Moscow University's President, *in order to eliminate the illiteracy in the field of information security, it is required to bring together the efforts of science, education, media, businesses, and communities of Internet users. Sciences and education hold the first place in this combination, which should provide the tools to solve the problem: evidence-based recommendations, a wide range of special education programs, teaching methods, educational, scientific and popular literature.*

Thank you for your attention!

---

1 Source: https://www.cisco.com/c/en_us/about/press/press-releases/2016/02-03b.html

2 https://www.gartner.com/newsroom/id/3598917

3 Source: https://www.cisco.com/c/ru_ua/about/press/2017/05-30.html

4 Source: https://www.itu.int/net4/ITU-D/idi/2017/

5 See National center of Incident readiness and Strategy for Cybersecurity // http://www.nisc.go.jp/eng/

6 See http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf

7 Source: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

8 See: https://club.esetnod32.en/news/novosti _ eset/igrushki - shpiony/

9 Cyberattacks targeting Japan networks hit a record of 128.1 billion in 2016. https://www.japantimes.co.jp/news/2017/02/08/national/crime-legal/cyberattacks-targeting-japan-networks-hit -record-128-1-billion-2016 / #. Wgi6SrhR37k

10 http://www.securitylab.ru/news/488795.php / https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf

11 OV Khramov. http://www.scrf.gov.ru/news/allnews/2164/

Commentators:

Keiko Kono

(Senior Research Fellow, National Institute for Defense Studies)

Sovereignty and Non-Intervention in Cyberspace: Consideration by Analogy to Past Russian Claims

I. Introduction

It is confirmed in the 2015 Report of UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security that the existing international law, in particular the fundamental principles embodied in the United Nations Charter, are applicable to cyber operations by States.[1] But experts disagree on how they could be applied to the specific phases of operations unique to cyber activities. For example, Western States recognize that *jus ad bellum* (regulation on use of force by and right of self-defense of States) applies to the cyber context in the framework of NATO[2] and G-7,[3] while Russia and China contend that information and communication technologies (ICT) are not a weapon and deny its applicability.[4] There seems a long way to go before both sides will be able to reach a consensus on this issue.

The purpose of this paper is to focus on several topics that all States are assumed to consider as grave concerns and assess to what level that measures for States afflicted by cyber operations of other States would be acceptable for Russia as well as Western States. I will start by reviewing why an increasing number of States advocate the principle of prohibiting cyber intervention with the domestic affairs of foreign States. It is well known that the USSR and other States insisted on the sovereign right to control any information entering its territory in the 1970s when international direct television broadcasting by satellite became common. Their argument at that time is now reflected in the current cyber discussion. The USSR also suggested the possibility of retaliatory measures against unjust broadcasts by other States that infringe on the sovereign right of receiving States. This provides an interesting point when considering the consequences of illegal cyber activities by States, as these retaliatory measures advocated by the USSR at the time can implicate that possible countermeasures by a victim State can be justifiable in the cyber context as well.

II. Principle of Prohibiting Cyber Interference

This issue of cyber sovereignty is not new, if we recall the similar US-USSR conflict since the early 1970s in relation to international direct television broadcasting by satellite. At that time, the USSR advocated the State's sovereign right to control broadcasted program content, while the US strongly asserted free flow of information. This situation is basically the same as the current dispute between States regarding cyber sovereignty.

1. The Assertion of Sovereignty of Receiving States for International Direct Broadcasting by Satellite

The USSR submitted to the UN General Assembly in 1972 a draft Convention on Principles Governing the Use by States of Artificial Earth Satellites for Direct Television Broadcasting.[5] In that document, the USSR made the following assertions. First, that "the generally recognized principles of international law, including the United Nations Charter and the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," could be applied to newly emerged direct television broadcasting by means of artificial earth satellites (Article 2). Next, States shall not broadcast any television programs that are "interfering in the domestic affairs or foreign policy of other States" by means of artificial earth satellite (Article 4), and "direct television broadcasting by means of artificial earth satellites" can be carried out by a State "only with the express consent of" the receiving States (Article 5).

Transmission of television programs without such consent "shall be regarded as illegal" (Article 6), and a victim State of illegal television broadcasting "may employ the means at its disposal to counteract" the illegal act by other States (Article 9). Although the draft Convention did not refer to any concrete measure that a victim State may take in retaliation, experts at that time suggested that it could mean not only broadcast jamming, but also to destroy the satellites.[6]

In November 1972, the UN General Assembly Resolution 2916 was adopted with 102 votes in its favor.[7] The resolution recognized the need to elaborate principles for direct television broadcasting with the aim of ultimately concluding an international agreement. The United States cast the sole dissenting vote and opposed the making of international conventions on this issue, noting that the sovereignty of States and the free flow of information should "complement rather than conflict with one another," but that this concept was not fully recognized in the draft resolution.[8]

Ten years after, in 1982, the UN General Assembly adopted the "Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting" as the Resolution 37/92.[9] The provision on retaliatory measures by a State afflicted by illegal direct broadcasting in Article 9 of the draft Convention submitted by the USSR in 1972 was not included in this Resolution. However, most of the Western States felt that the Resolution excessively protected the sovereign right of the receiving State, and 13 States voted against, while 13 States abstained from voting.[10] This Resolution supported the basic principles proposed by the USSR in 1972. For example, a State which intended to conduct an international direct television broadcasting services "shall without delay notify the proposed receiving State" and "shall promptly enter into consultations with any of those States which so requests" (paragraph 13) and an international direct television broadcasting satellites service "shall only be established...on the basis of agreements and/or arrangement" concluded among States involved in the matter (paragraph 14). In addition, this "agreement and/or arrangement" has been interpreted as including not only technical aspects, but also non-technical issues such as program content regulation. Following these moves, some academic scholar assessed that it is quite difficult to prove that the principles of free information for individuals and free distribution of information between States, as according to general international law, apply to recognizing the right for a State to engage in international broadcasting services and prohibiting a receiving State from obstructing it.[11] If this assessment is correct, it means that States can obstruct and regulate incoming information in the name of its sovereign right.

2. Russian and Chinese Views on Sovereignty in Cyberspace

The conflicting views between the US and the USSR on international direct television broadcasting by satellite have been carried over to the current discussion on cyberspace, in which the US insists on free flow of information, while Russia and China claim the right to control the influx of information to their territories that may disturb public order. Russia and China are concerned that the Western States may send a massive amount of information that is not favorable to their governments, and therefore, they have been intent on blocking that detrimental information. From their point of view, cyberspace should be considered a kind of national territory where the government can exercise its sovereign right to control all information,[12] and it would make sense to conclude an international agreement on this issue so that international society understands this.

Russia and China have taken a more sophisticated approach in their draft International Code of Conduct for Information Security that was submitted to the UN Secretary General in 2015[13] as an update of the first draft in 2011. The 2015 draft touches upon the human rights to seek, receive and impart information, in addition to principles to respect the sovereignty of States by referring to the International Covenant on Political and Civil Rights of 1966. The Covenant recognizes that such human rights are subject to certain restrictions when necessary for the protection of national security or of public order, or of public health or morals in Article 19 (3). Although China has not ratified the Covenant, this provision may serve as a framework for Russia and China to justify their control on information within their territory. The principle of free flow of information that the US has asserted in the context of human rights since the 1970s has not always been absolute when it comes to relationships with other States. Consequently, even if the US and other Western States assert that it is unacceptable for Russia and China to regulate information in cyberspace, such an assertion may not be opposable to them.

On the other hand, the alleged Russian disinformation operations to interfere with elections in the US and Europe over the past few years have made Western States reconsider the risk that free flow of information could be abused, and inherent government functions such as elections could be obstructed by foreign States. As the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* pointed out, there has not been a consensus on the meaning of the principle of sovereignty in cyberspace among the States,[14] but there is no doubt that the States must accept the basic principle advocated by the USSR that the communication activities of States must not interfere with the internal issues of other States. To conclude an international agreement is not a realistic approach, in light of the failed initiative for international direct television broadcasting by satellite. Moreover it may not be necessary because States can accumulate state practices by confirming principles prohibiting cyber interference with like-minded States in the framework of G-7 or other regional organizations, which would greatly contribute to the establishment of international law.

3. Applicability of Countermeasures by a Victim State in the Cyber Context

As mentioned before, the USSR asserted in its 1972 draft UN Convention that a State afflicted by illegal direct television broadcasting could take retaliatory measures at its disposal. It is widely known that the USSR was indeed jamming detrimental radio broadcasting from Western States during the Cold War.[15] However, destroying an artificial satellite could amount to a use of force as prohibited under Article 2(4) of the UN Charter.

Leaving aside the question of illegality of such retaliatory measures, I would like to focus on the fact that the USSR has traditionally taken countermeasures in response to harmful broadcasting services by other States. Cyber operations by States carry rights and obligations, and therefore, the law of State responsibility must obviously be applied. There is no logical reason for cyber countermeasures and necessity to be excluded. A victim State of illegal cyber operations can resort to various means of redress or countermeasures, including, but not limited to, criminal indictment of the offenders or economic sanction on the responsible State, if the victim State has been able to identify the offending persons or State. Russia should also support this idea, considering its own history.

However, cyber activities should be distinguished from other information and telecommunication techniques traditionally employed by States such as radio and satellite broadcasting, as they may function as a weapon that physically destroys things. A media article once reported that the US forces engaged in a "left of launch" cyberattack strategy to thwart missile launches by North Korea.[16] It could be argued that such a US operation was justified as a countermeasure to repeated threats of force and other internationally illegal acts by North Korea. Yet, it still remains unclear whether cyberattacks could meet other requirements of countermeasures, especially when they may cause physical and functional harm to critical infrastructures of other States. An answer to that question will depend on how we define the use of force in the cyber context, because a countermeasure in general should not amount to the use of force, as agreed by many States.[17] Besides, before resorting to a countermeasure, the victim State must be able to identify the State that committed the wrongful act. Such identification is the most difficult part in seeking State responsibility and individual liability in the field of cyber operations.

III. Conclusion

According to a prominent expert who was involved in the drafting of the *Tallinn Manual 2.0*, the element of coerciveness must accompany a cyber intervention, "which attempts to prevent a State from conducting its domestic affairs and foreign relations in conformity with its own choices within the limits of international law."[18] But, there are divergent views as to whether the series of alleged Russian election interference constituted a prohibited intervention or not.[19] In regards to international television direct broadcasting by satellite, this was not a coercive activity from the Western perspective, yet the USSR criticized it as "external interference."[20] This is why the USSR believed it was critically important to refer to the principle of non-intervention in its draft Convention submitted in 1972. Now that States share the common concern that their election and other government functions could be disrupted or threatened by malicious disinformation campaigns and cyberattacks from foreign States, many presumably see the benefit in prohibiting this legally. It would be best for not only the Western States, but also for Russia and China to join in active dialogue regarding this

new aspect of the principle of non-intervention in the context of international law. If this is not a feasible option, States can accumulate relevant national practices with like-minded States that would contribute to the development of an international customary law. Determining what types of actions shall be deemed illegal according to international law is an indispensable prerequisite for a victim State to clarify the responsibility of the responsible State.

---

1 UN Doc., A/70/174, July 22, 2015.

2 Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 5, 2014, available at https://www.nato.int/cps/en/natohq/official_texts_112964.htm

3 "G7 Principles and Actions on Cyber," G7 Ise-Shima Summit, May 26-27, 2016, available at http://www.mofa.go.jp/mofaj/files/000160279.pdf

4 Andrey Krutskikh and Anatoly Streltsov, "International Law and the Problem of International Information Security," *International Affairs: A Russian Journal of World Politics, Diplomacy and International Relations*, Vol. 60 (2014), pp. 64-76.

5 Request for the Inclusion of a Supplementary Item in the Agenda of the Twenty-Seventh Session, Preparation of an International Convention on Principles Governing the Use by States of Artificial Earth Satellites for Direct Television Broadcasting, Letter dated 8 August 1972 from the Minister for Foreign Affairs of the Union of Soviet Socialist Republics addressed to the Secretary, General, UN Doc., A/8771, August 9, 1972.

6 "The Control of Program Content in International Telecommunications: A Discussion of General Principles," *Columbia Journal of Transnational Law*, Vol. 13 (1974), p.51; Sharon L. Fjordbak, "The International Direct Broadcast Satellite Controversy," *Journal of Air Law and Commerce*, Vol. 55 (1990), pp. 910 and 915.

7 UN Doc., A/RES/2916(XXVII), November 9, 1972.

8 UN General Assembly, 2081st Meeting Record, UN Doc., A/PV. 2081, November 9, 1972, p. 5, para.47 and 48.

9 UN Doc., A/RES/37/92, Annex: Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, December 10, 1982.

10 Soji Yamamoto, "Transborder Data Flow and Legal Function of Telecommunication Sovereignty," *Jurist*, Special Edition (1984), p. 71 (in Japanese).

11 Ibid., pp. 71-72.

12 Doctrine of Information Security of the Russian Federation (Unofficial Translation), Approved by Decree of the President of the Russian Federation, No. 646 of December 5, 2016, The Ministry of Foreign Affairs of the Russian Federation website, available at http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

13 UN Doc., A/69/723, January 13, 2015.

14 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), Part 1, Section 1.

15 John B. Whitton, "Cold War Propaganda," *American Journal of International Law*, Vol. 45 (1951), pp. 151-153.

16 "The U.S. Wants to Stop North Korean Missiles before They Launch. That May Not be a Great Idea," *The Washington Post*, March 15, 2017, available at https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/15/the-u-s-wants-to-stop-north-korean-missiles-before-they-launch-that-may-not-be-a-great-idea/?noredirect=on&utm_term=.c142927843a0

17 International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts (2001), Article 50 (1)(a).

18 Terry D Gill, "Non-Intervention in the Cyber Context," in Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013), p. 232.

19 Professor Schmitt describes the alleged Russian hacking of servers of the US Democratic National Committee (DNC) as a grey zone surrounding coercion. Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online*, Vol. 42 (2017), p. 8.

20 UN Doc., A/PV. 2081, p. 4, para. 37.

Commentators:
Yu Koizumi
(Special Researcher, Institute for Future Engineering)

The Prospects for Japan-Russia security cooperation in cyberspace

Preface: Different understandings of common domain

The author's comments during this symposium fall into two broad categories.

First, interest on the Japan side focuses on "cybersecurity," while the priority on the Russian side is "information security." Thus, there are conceptual gaps between Japan and Russia.

Second, the Internet has become an essential domain for both ordinary life and security, but unlike other domains--land, sea, air, space--it is an artificial construct. Most of the infrastructure that supports this artificial domain was built by Western countries, and that has become a point of considerable concern for Russia in recent years. It is also a point that Japan, as a member of the Western world, does not fully understand, and is therefore another point of difference between Japan and Russia.

In other words, while Japan and Russia talk to each other about Internet security, there are fundamental differences in how they understand it. This paper explores these two points in a bit more depth as an attempt to bridge the understandings of Japan and Russia.

Russia's concept of "information security"

Japan's primary interest in cybersecurity is to prevent the unlawful use of cyberspace. The major threats envisioned are things like the large theft of e-money discovered in 2018, and past compromises of personal information. Other important issues in cybersecurity for Japan are to prevent cyberattacks from damaging Internet communications functions or causing social infrastructure to become dysfunctional.

In that sense, the security of cyberspace is obviously an important component of Russia's security policy as well. The major difference between Russia and Japan is that cybersecurity for Russia consists of the higher-level concept of "information security." A detailed reading of documents from the Russian government on security policy makes it clear that the country's security community is concerned with more than just a simple information theft and cyberattacks. Cyberspace is an information channel far better at propagating information than anything the past, but in spite of this, is not fully under state control; this is the focus of the Russians.

Cyberspace is more than just a medium for cyberattacks and illegal transactions through the "dark web" (for example, stolen e-money and illegal drugs), it is also a medium in which information uncomfortable to the Russian government circulates freely. Some examples of this information include criticisms by foreign governments of the military intervention in Ukraine and Syria, criticisms of the Putin administration by opposition parties, and religious and racial extremism. From the Russian government's point of view, the distribution of this kind of information constitutes an "information war" by enemy forces and must therefore be appropriately managed (selected, restricted, etc.) by the Russian government itself.

In contrast, Japan has freedom of speech that allows criticism of the government and state policy, and it would, in all likelihood, be impossible to reach a social consensus that the state should

intervene in some form. Nonetheless, interest has grown rapidly in Japan over the past few years on the question of how to handle statements that fan religious and racial discrimination. How far the state should intervene in the distribution of information is perhaps a topic that experts from Japan and Russia could discuss.

Internet as artifact: Russia's unease

It is easy to forget that the Internet is an artifact, a man-made construction. If the communications lines are cut off or the server loses power, the Internet disappears. Obviously, the infrastructure supporting the Internet has multiple layers of redundancy and cannot be brought down so easily. At the very least, it would be virtually inconceivable for Japan to become completely isolated from the Internet; it survived even the Great East Japan Earthquake of 2011.

Russia, however, does not place as much faith in the robustness of the Internet. DNS root servers and other core Internet infrastructure are in the hands of the United States and other "Western" powers, and Russia is unable to completely eliminate the potential that its Internet access could be artificially cut off for political reasons. It is reported that the Russian government has been increasingly concerned about this kind of situation since the Ukraine crisis of 2014 in particular, and that summer, the Ministry of Telecom and Mass Communications conducted exercises positing the country's shut off from the global Internet. This is also why "Digital Economy Doctrine" and other policy documents from the Russian government emphasize the autonomy of communications lines and other Internet infrastructure.

Japan, as a member of the Western side, does not share Russia's concerns in this regard. However, a fracturing of the global Internet is not desirable for Western society either. While we cannot and would not prevent Russia from increasing the autonomy of its Internet as an extraordinary means in times of emergency, we can at least work to maintain an open, connected Internet during normal times. What can Japan do to further this? This could also be a topic for discussion between Japan and Russia.

Editorial postscript

From the preparation of the Cybersecurity Symposium cohosted with the Information Security Institute of Lomonosov Moscow State University (IISI) to the compilation of this inaugural booklet, a tremendous amount of assistance was provided by Hiroyuki Fujimaki, Deputy Director of the Strategic Peace and International Affairs Research Institute of Tokai University and Assistant Professor, Department of Political Science, School of Political Science and Economics. Looking back, as someone with no expertise in the areas of cybersecurity and Russia, this symposium was a huge task for me. It was Professor Fujimaki, with his experience in researching international relations in Eurasia and his network within Moscow State University, who enabled me to fulfill my minimum responsibilities.

Although this was not published in the booklet, according to Professor Fujimaki, a delegation from China attended a symposium hosted by Moscow State University at the Russian Ministry of Foreign Affairs he attended last December. While what has been described as a new Cold War between the US and China over supremacy in high-tech technology and telecommunications infrastructure, it looks as though, for the time being at least, that Russia and China are in solidarity. From a long-term perspective, I believe that Japan and Russia should build a stronger cooperative relationship in response to China, which is seeking to further its own interests in Northeast Asia and the Arctic Ocean. The difficult Northern Territories issue remains an obstacle in concluding a peace treaty between Japan and Russia, but I am also fully aware of the importance of our network with Moscow State University and Far Eastern Federal University. I hope that we can continue to deepen academic exchanges in the future. For the cybersecurity symposium, Ikuo Misumi, Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity, Cabinet Secretariat (position at the time), kindly provided us guidance on everything from basic cybersecurity knowledge to building a research and education system. Thank you again for doing this. Finally, I would also like to express my sincerest gratitude to Katsumi Tashiguchi of Tokai University Press, for enduring significant delays in manuscript processing and compilation on my part as I found myself pressed for time trying to also play the role of journalist. Thank you.

Yoshimasa Suenobu
February 3, 2019