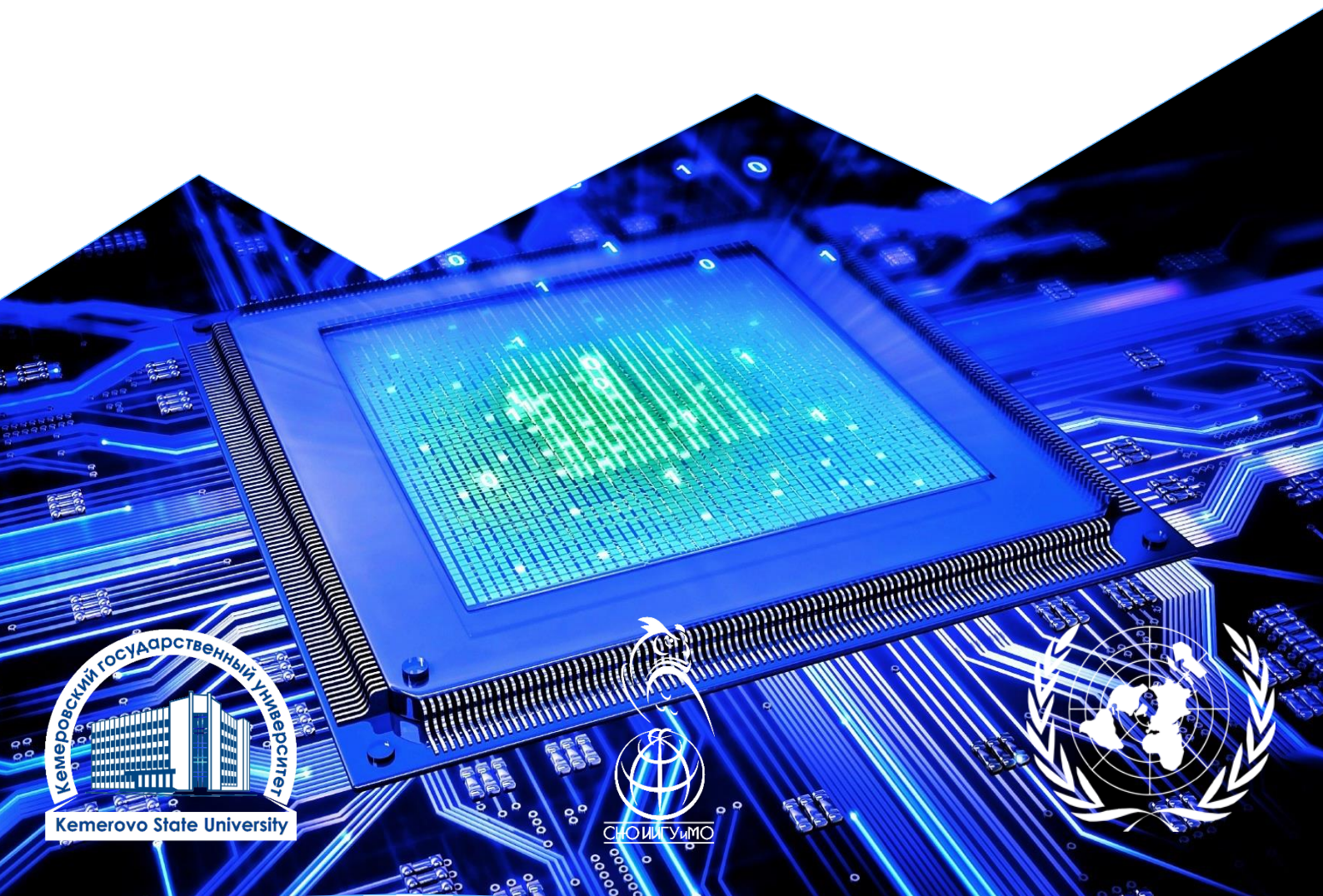
THE KEMEROVO INTERNATIONAL MODEL UN 2016

ENSURING INTERNATIONAL INFORMATION SECUTIRY

COMMITTEE ON INFORMATION: EXPERT REPORT



Welcome speech of expert.

Distinguished delegates,

! I am delighted to welcome you at this session of the Committee on Information. This time, you and I have to focus on the issue of cybersecurity.

As an expert of the Committee on Information, I invite you to take part in the meetings of our committee. Maintenance of international cybersecurity is the main obligation entrusted to us. In this regard, you are to discuss a very exciting agenda: "Ensuring International cybersecurity". For our part, we will try to do everything possible to make this model the most memorable event of your student life.

The emergence and spread of the Internet has brought the discussion on information security issues to the next level. Such issues are especially relevant nowadays due to development of cyber technologies and rise in cybercrime.

Freedom of information causes threats that are hard to resist at the current level of development of the Internet security technologies.

First of all, it is a sharing of prohibited content. The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances, these communications may be legal.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

Secondly, it is the activation of hacking and insecurity of storage and dissemination of information. The events related to them, are increasingly announced in the world news. The threat is incredibly serious - and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Both private and public sector networks are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data, and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators.

Internet was supposed to unite the humankind and destroy all barriers. The spread of extremist information is a great threat for this, because such information leads to enmity and obstacles' growth in intercultural and other dialogues.

The ISIS especially succeeded and penetrated into all social networks, spreading its extremist ideology everywhere. Sometimes the dissemination of such information turns into information warfare among the political forces or even states, forcing aggression on both sides.

Criminals use the internet particularly for money-laundering, weapons, drugs and child pornography trade. Terrorists recruit new supporters online and coordinate their attacks. Hackers all over the world use the Internet for their purposes, usually with the aim to enrich themselves, making storage and dissemination of users' information unsafe. Even politicians are vulnerable to information leakage, as shown by the recent pre-election scandal in the United States.

This makes people distrust the Internet as an efficient way of communication. This forces the states control the Internet too, often violating the rights of their citizens. State restrictions on use of the Internet in some countries, are no less serious threat to the process of globalization and intercultural dialogue.

I hope that during the interesting meetings you, distinguished delegates, will be able to adopt such a resolution, which could deal with the issue of cybersecurity and human right to information, would have laid the mechanisms for effective implementation of Committee resolutions and which principles would be unanimously accepted by all countries of the world.

I believe that these days will be memorable for you, and you will not only learn a lot about world politics, learn how to speak in public in a foreign language, but also find new friends.

Have a good and constructive Model!

Yours faithfully,
Committee on information expert
Of Kemerovo Model UN 2016
Andrew Antipov

I. UN and information security

The Universal Declaration of Human Rights was adopted by the United Nations General Assembly on 10 December 1948. Its nineteenth article states: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". Over 95 countries around the world have implemented some form of freedom of information legislation. Sweden's Freedom of the Press Act of 1766 is the oldest in the world. Most of such laws were passed in 80's and 90's, when the Internet became widespread. However, we note with regret that today's world is far from a consensus on the issue, because every state has to restrict the right to information severely to ensure the security and to combat crimes, especially cybercrimes.

The UN often highlighted information issues. Especially for this under General Assembly resolution 33/115 C of 18 December 1978 the Committee to Review United Nations Public Information Policies and Activities was established. At its 34th session, the General Assembly decided to maintain it.

In its resolution 34/182 of 18 December 1979, the General Assembly outlined the mandate of the Committee on Information as follows:

1. To continue examining United Nations public information policies and activities, in the light of the evolution of international relations, particularly during the past two decades, and of the imperatives of the establishment of the new international economic order and of a new world information and communication order;

2. To evaluate and follow up the efforts made and the progress achieved by the United Nations system in the field of information and communications; and

3. To promote the establishment of a new, more just and more effective world information and communication order intended to strengthen peace and international understanding and based on the free circulation and wider and better-balanced dissemination of information and to make recommendations thereon to the General Assembly.

The issue of information security has been on the UN agenda since the Russian Federation first introduced a draft resolution in 1998 on the subject in the First Committee of the UN General Assembly. It was adopted without a vote by the General Assembly as resolution 53/70. Since that time there have been annual resolutions calling for the views of UN Member States on the issue of information security.

Groups of Governmental Experts

There have been four Groups of Governmental Experts (GGEs) that have examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them.

The first 15-member Group was established in 2004 but did not agree on a substantive report. Information on the procedural matters of the Group's work was published as UN document A/60/202. Disagreement among the experts emerged primarily over two substantive policy issues. The first issue was the question of the impact of developments in information and communications technologies (ICTs) on national security and military affairs. While there was general agreement regarding the importance of such developments, consensus could not be found on the amount of emphasis to be placed on this concern, and whether or not to include language that stressed the new threats posed by State exploitation of ICTs for military and national security purposes. The second issue was the question of whether the discussion should address issues of information content or whether it should focus only on information infrastructure. There was particular disagreement regarding the claim that trans-border information content should be controlled as a matter of national security. Other areas of disagreement arose on proposals for capacity-building and technology transfer to developing countries.

The second 15-member Group was established in 2009. A successful GGE report was issued in 2010 (A/65/201). The 2009/2010 GGE recommended the following in its report:

1. Dialogue on norms for State use of ICTs to reduce risk and protect critical infrastructure;

2. Confidence-building and risk-reduction measures, including discussion of ICTs in conflict;

3. Information exchanges on national legislation and national ICT security strategies, policies and technologies;

4. Capacity-building in less-developed countries;

5. Elaboration of common terms and definitions on information security.

GGE in 2012/2013

In 2011, the General Assembly unanimously approved resolution 66/24, in which it called for a follow-up GGE. This third Group had three one-week meetings in 2012/2013. Ms. Deborah Stokes (Australia) was unanimously elected as Chair of the Group.

The Group's report (A/68/98*) was submitted to the UN General Assembly in June 2013.

The Group agreed on the following:

1. International law, in particular the UN Charter, is applicable to the cyber-sphere and is essential for an open, secure, peaceful and accessible ICT environment.

2. State sovereignty applies to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

3. State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms.

4. States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-State actors for unlawful use of ICTs.

5. The UN should play an important role in promoting dialogue among Member States.

Secretary-general claimed in his foreword to the report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, June 2013:

"I appreciate the report's focus on the centrality of the Charter of the United Nations and international law as well as the importance of States exercising responsibility. The recommendations point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security".

GGE in 2014/2015

On 27 December 2013, the UN General Assembly unanimously adopted resolution 68/243 which requested the Secretary-General to establish a new GGE that would report to the General Assembly in 2015. The new GGE, with 20 experts, held four meetings between July 2014 and June 2015. Experts from the following Member States participated in the GGE: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russian Federation, Spain, United Kingdom and United States of America. Mr. Carlos Luís Dantas Coutinho Perez (Brazil) chaired the Group.

The Group agreed on a substantive consensus report to be sent to the Secretary-General on norms, rules or principles of the responsible behaviour of States in the cyber-sphere as well as confidence building measures, international cooperation and capacity building which could have wider application to all States. It also addresses how International Law applies to the use of information and communications technologies and also makes recommendations for future work. It will be released later this summer and presented to the General Assembly in September.

UN Office for Disarmament Affairs

The Office for Disarmament Affairs has provided substantive support to the expert Groups and has acted as the secretariat assisting in the preparation of the Group's reports

II. Cybercrime and cybersecurity

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:

1. Advanced cybercrime (or high-tech crime) includes sophisticated attacks against computer hardware and software. About 40 million people in the United States, roughly 15 percent of the population, has had personal information stolen by hackers, it said, while high-profile breaches affected 54 million people in Turkey, 16 million in Germany and more than 20 million in China.

The collective impact is staggering. Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and emergency services around the world.

Who is behind such attacks? It runs the gamut - from computer geeks looking for bragging rights, to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets, to spies and terrorists looking to rob our nation of vital information or launch cyber strikes.

2. Cyber-enabled crime – many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism.

Today, these computer intrusion cases - counterterrorism, counterintelligence, and criminal - are the paramount priorities of national and worldwide cyber programes because of their potential relationship to national security.

The changing nature of cybercrime

New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars. Cyber crime costs the global economy about $445 billion every year, with the damage to business from the theft of intellectual property exceeding the $160 billion loss to individuals from hacking, according to research published by the Center for Strategic and International Studies (CSIS).

In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale.

Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging.

National federal agencies succeeded in the fight against cybercrime. For example, the FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. Nevertheless, the world community joined efforts to fight cybercrime. A key role in this regard belong with the INTERPOL. INTERPOL is committed to the global fight against cybercrime, as well as tackling cyber-enabled crimes.

Most cybercrimes are transnational in nature, therefore INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale.

INTERPOL is committed to being a global coordination body for the detection and prevention of digital crimes through the INTERPOL Global Complex for Innovation (IGCI) in Singapore. This cutting-edge research and development facility, which opened in 2014, leverages global cyber-expertise from law enforcement and key private sector partners.

INTERPOL is uniquely positioned to advance the fight against cybercrime on a global scale through proactive research into emerging crimes, the latest training techniques, and development new policing tools.

Sources:

1. FBI. Addressing Threats to the Nation's Cybersecurity: https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view

2. NATO Cooperative Cyber Defence Centre of Excellence. United Nations: https://ccdcoe.org/un.html

3. General Assembly Resolutions: http://www.un.org/en/sections/documents/general-assembly-resolutions/index.html

4. United Nations General Assembly. Sixty-fifth session. Item 94 of the provisional agenda. Developments in the field of information and telecommunications in the context of international security: http://www.un.org/ga/search/view_doc.asp?symbol=A/65/154

5. United Nations General Assembly. Sixty-sixth session. Item 93 of the provisional agenda. Developments in the field of information and telecommunications in the context of international security: http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152 http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152/Add.1

6. United Nations General Assembly. Sixty-seventh session. Item 90 of the provisional agenda. Developments in the field of information and telecommunications in the context of international security: http://www.un.org/ga/search/view_doc.asp?symbol=A/67/167

7. United Nations General Assembly. Sixty-eighth session. Item 94 of the preliminary list. Developments in the field of information and telecommunications in the context of international security: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156 http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156/Add.1

8. United Nations General Assembly. Seventeeth session. Item 93 of the preliminary list. Developments in the field of information and telecommunications in the context of international security: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172

9. United Nations General Assembly. Seventy-first session. Item 93 of the preliminary list. Developments in the field of information and telecommunications in the context of international security: http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172