

## **Developments in the field of information and telecommunications in the context of international cyber security**

Intensive development of information and communication technologies (ICTs) and their wide use in all spheres of human activity have accelerated post-industrial development and the building of a global information society.

ICTs have become a driving force of social development. The global information infrastructure provides unprecedented opportunities for communication among people, their socialization and access to information. Individuals, society and the state depend on the stability and reliability of the information infrastructure.

However, ICTs could enable a fundamentally new and effective means to disrupt or destroy a country's industry, its economy, social infrastructure and public administration. ICTs have the potential to be a means of combat capable of achieving goals related to inter-state confrontation at the tactical, operational and strategic levels. In this way ICTs gain the characteristics of a weapon "designed to defeat an enemy in combat". The potential destructive power of so-called "information weapons" will increase as ICTs develop further and as the information infrastructure of society evolves. This power will be magnified as military equipment and weapons are increasingly integrated with—and reliant on—ICTs.

These concerns are neither new nor limited to just one country or region. For example, the need to encourage the beneficial uses of ICTs and minimize the negative consequences was expressed in the 1998 joint statement of the Presidents of the Russian Federation and the United States "Common Security Challenges at the Threshold of the Twenty-First Century", which highlighted "the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place, which is a serious challenge to ensuring the future strategic security interests of our two countries."

### **Initial international efforts**

Concerned about the emergence of new threats to peace and security, the Russian Federation has been promoting the issue of information security at the international level for nearly a decade. On 23 September 1998, I.S. Ivanov, Minister of Foreign Affairs of the Russian Federation, submitted a letter to the UN Secretary-General requesting circulation of a draft resolution on information security. A resolution entitled "Developments in the field of information and telecommunications in the context of international security" was then adopted by consensus at the Fifty-third Session of the General Assembly.

### **Icts and international security**

The resolution called upon UN Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security. The resolution also invited all Member States to inform the Secretary-General of their views and assessments of the following issues:

- a general appreciation of the issues of information security;
- the definition of basic notions related to information security, including unauthorized
- interference with or misuse of information and telecommunications systems and information resources; and the advisability of developing international principles that would enhance the security
- of global information and telecommunications systems and help to combat information terrorism and criminality.

The Secretary-General was requested to report to the Fifty-fourth Session of the General Assembly. The report of the Secretary-General reflected the acknowledgement of the problem of international information security, as well as its complexity and multiple facets.

Based on submissions from Australia, Belarus, Brunei Darussalam, Cuba, Oman, Qatar, the Russian Federation, Saudi Arabia, the United Kingdom and the United States, the report highlighted the different priorities accorded by states to individual aspects of the issue as well as different approaches to the issue taken at the national and, especially, international levels.

Following this initial exploration of views, at the Fifty-fourth Session of the General Assembly the Russian Federation proposed a new draft resolution, where for the first time the military potential of ICTs was by name put directly under the spotlight. This resolution was adopted without a vote on 1 December 1999.

In May 2000, with the objective of furthering discussion on the issue, the Russian Federation submitted to the UN Secretariat draft principles concerning international information security. These materials facilitated the adoption at the Fifty-fifth Session of the General Assembly of a resolution that noted the advisability of "examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems".

In 2001, UN Member States agreed to establish a Group of Governmental Experts (GGE), commencing work in 2004, to review existing and potential threats in the field of international information security and possible measures to address them as well as to examine international concepts aimed at strengthening the security of global information and telecommunications systems. Thus, for the first time at the international level, a political decision was made to move from discussion on the issue to practical action. In April 2003 the Russian Federation submitted to the UN Secretariat a new contribution entitled "Issues Connected with the Work of the Group of Governmental Experts on Information Security", which contained the Russian vision of organizational, practical and substantial aspects of the group's work. In particular, it was noted that it is necessary to seek a multilateral, mutually acceptable, international legal document aimed at strengthening the universal character of an international information security regime.

The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security met in 2004 and 2005, tasked with the preparation of a draft report for the UN Secretary-General. Even though the group undertook a substantial amount of work, it was unable to reach consensus on a draft report. The main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of "hostile" use of ICTs for politico-military purposes.

However, the work of the GGE was not in vain. It successfully raised the profile of the relevant issues on the international agenda. The preliminary exchange among states of their opinions on the most complicated aspects of these issues has been particularly fruitful. The importance accorded these topics is evident in the fact that the UN General Assembly has decided to continue studying this problem.

Various aspects of the issue of information security have also been taken under consideration in other international and regional forums, such as the International Telecommunication Union, the World Summit on the Information Society, and the Council of Europe. In addition to the resolutions mentioned above, the General Assembly has addressed other aspects of the ICT issue, such as creating a global culture of cybersecurity and the protection of critical infrastructures.

### **Deliberately Influencing another state's vital structures**

The use of ICT weapons would be particularly dangerous when used against military and civilian facilities and state systems and institutions, the disruption of the normal functioning of which could constitute a direct threat to national security.

Unauthorized penetration into control systems, for example that of a country's power grid, could bring about total paralysis of a country's infrastructure. Imagine the disastrous environmental risks if the chemical, biological or fuel industry were thus attacked, or the catastrophic consequences if a nuclear power station were involved.

Another critical sector is that of credit and finance. The unauthorized transfer or outright theft of bank resources, the "closing" of accounts and, in particular, mounting electronic attacks to block the computer networks of central banking institutions, could obviously not only create crisis situations in that particular area but also bring about the country's economic collapse or jeopardize its relations with other countries.

Massive destruction of the telecommunications infrastructure through the use of ICTs would amount to an attack on a state's control and decision-making systems.

An ICT attack on anti-aircraft, anti-missile and other defence communication and control systems would leave a state defenceless before a potential aggressor, thereby depriving it of the possibility to exercise its legitimate right of self-defence.

Targeting the communication, control and transportation systems of emergency response services could increase the loss of life and property in times of man-made or natural disaster.

Databases and other information resources of law enforcement bodies could be distorted or completely obliterated, which would gravely interfere with the fight against crime and the maintenance of law and order.

### **Information warfare and international law**

There is no doubt that information weapons can be used in practice. Some armed forces are already preparing special units for military operations using ICTs. The US Air Force, for example, has been quite open about its plans and is in the process of setting up a dedicated command—the Air Force Cyberspace Command.

Further efforts by the international community to address the threat of hostile use of ICTs will depend on whether existing international law is seen as adequate to ensure international information security. This was affirmed by the 2004 International Expert Conference on Computer Network Attack and the Applicability of International Humanitarian Law, and within the discussions of the UN Group of Governmental Experts in 2004 and 2005.

The opportunities for carrying out massive attacks mean that ICTs could become a fundamental instrument of inter-state conflict.

### **the Issue of territory**

The absence of a clear definition of "territory" in relation to cyberspace contributes to the gaps in international security law. Paragraph 4 of Article 2 of the UN Charter requires that all states shall refrain from the threat or use of force against the territorial integrity of another state. It is implied that there exists a physical territory subject to the state's jurisdiction and a formal border separating that territory from other states. However, there are no such concepts as national border and territory in the information sphere. A state could consider the entire global information infrastructure (or a portion

thereof) to be its own territory, claim jurisdiction over the relevant elements of the information infrastructure and, on this basis, take action to defend these elements.

### **Identifying the attacker**

Another complicating factor is how to reliably identify the agent of an information attack. It is technically challenging to localize the physical place from which such an act originates. But even if the origin of an attack can be localized within a particular state, it would be challenging to determine whether the attacker was acting in an individual capacity, or on behalf of a criminal organization, the government or armed forces. In such cases, the presumed perpetrator of an aggressive act could be falsely accused instead of truly identified.

### **Protecting critical Infrastructure facilities**

International law does not specifically cover the use of ICTs as a means of coercive pressure on an opposing state.

According to the Laws and Customs of War on Land introduced by the Hague Convention of 18 October 1907, "the attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended is prohibited." Moreover, states party to the Convention are obliged to take "all necessary steps ... to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes." These rules aim to alleviate the unnecessary suffering of the civilian population and the wounded as a result of military operations.

To be able to apply these provisions to cyberspace, it would be essential to be able to "mark" in some way the information systems used to maintain the viability of critical social infrastructure facilities: both for individual facilities (including military and civil hospitals, bomb shelters, etc.) and entire regions (water supply, electrical grids, dams, etc.). In the physical world, some of these facilities (such as hospitals) display a distinctive sign—the red cross or red crescent—indicating their protected status. Such identifying signs are absent in cyberspace, nor do criteria exist for designating these systems as critical infrastructure.

---

#### SOURCES and useful Links

<http://www.unausa.org/Document.Doc?id=334> ( **very useful!!!!**)

<http://www.unidir.org/pdf/activites/pdf2-act82.pdf>

<http://www.unidir.org/pdf/articles/pdf-art2642.pdf>

**[http://www.un.org/ga/search/view\\_doc.asp?symbol=A/63/139](http://www.un.org/ga/search/view_doc.asp?symbol=A/63/139)** <sup>1</sup>

**<http://www.un.org/documents/ga/docs/56/a56164.pdf>** <sup>2</sup>

[http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN\\_resolution\\_57\\_239.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf) (Resolution 2003)

[http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN\\_resolution\\_58\\_199.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf) (Resolution 2004)

<sup>1</sup> **statements made (2008) by:** China, Cuba, Jordan, Libanon, Niger, Qatar

<sup>2</sup> **statements made (2001) by:** Bolivia, Sweden (On behalf of the States members of the EU that are Members of UN), Mexico, Philippines