

International information security: description and legal aspects

A.A. STRELTSOV

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.¹ In this way ICTs gain the characteristics of a weapon "designed to defeat an enemy in combat".² 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."³

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.⁴

A.A. Streltsov is Doctor of Engineering, Doctor of Law, professor, corresponding member of the Cryptography Academy of the Russian Federation, information security expert, and was a member of the Russian delegation at the meetings of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2004–2005).

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.⁵ 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,⁶ 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".⁷

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.⁸ 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.⁹ 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.¹⁰ A new group of governmental experts will commence work in 2009.

Over the last 10 years, various aspects of the issue of information security have 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.¹¹

International information security

Before addressing the question of whether existing norms of international law are sufficient to cope with the hostile use of modern ICTs, it is necessary to outline the area of study.

Information security is concerned with the threat of a state using ICTs to influence or attack the ICTs of another state. The hostile use of ICTs could generate situations considered as a threat to international peace and security.¹² Three aspects merit particular concern, each described briefly below.

INFLUENCING AND DAMAGING ANOTHER STATE'S INFORMATION RESOURCES AND TELECOMMUNICATIONS SYSTEMS USING ICTs

These include:

- electronic attacks or information attacks through electronic impulses to temporarily or permanently neutralize electronic installations or systems;
- destroying or altering the operational algorithm of ICT control systems;
- influencing, disrupting or halting information or communication flows through interference with the signal distribution environment;
- spreading disinformation or creating a virtual picture partially or totally misrepresenting reality in the communications sphere; or
- producing disorientation, loss of will power or temporary destabilization among the population.

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.

UNDERMINING A STATE'S ECONOMIC AND SOCIAL SYSTEMS AND PSYCHOLOGICAL MANIPULATION OF A POPULATION FOR THE PURPOSE OF DESTABILIZING SOCIETY

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

The deliberate use of information to damage an opponent is hardly new. Today, however, owing to the widespread use of and reliance upon ICTs, the potential for such misuse has greatly increased. The opportunities for carrying out massive attacks mean that ICTs could become a fundamental instrument of inter-state conflict. As described

in the contribution of the Russian Federation to the Secretary-General's 2001 report *Developments in the Field of Information and Telecommunications in the Context of International Security*:

Pressure arising out of the predominance of a limited range of information sources might be used for the deliberate creation of a negative psychological effect on a country's population as a whole or on the staff of critically important structures, administrative and government services and legislative bodies.

Causing people to feel unable to resolve their own problems, to mistrust the country's institutions or to feel hopeless, attacking their will power or provoking religious, ethnic or other conflicts undermines the foundations of the State and destabilizes society. Ultimately, such a situation could lead to antagonism between social groups, to civil war and to total disintegration of the State.¹³

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.¹⁴

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,¹⁵ and within the discussions of the UN Group of Governmental Experts in 2004 and 2005.

Ensuring international information security should be based on the principle of preserving existing international law (*jus ad bellum*), which regulates how threats to international peace and security are countered, and on international humanitarian law (*jus in bello*), which regulates the methods and means of warfare, protection of states that are not parties to the conflict, as well as of persons and objects that are or may be affected by the conflict.

In the international community's attempts to clarify this complex topic, there should be no attempt to diminish the legitimate right of self-defence of states to respond to hostile use of ICTs, just as they have the right to respond to a conventional weapon attack.

THE UN CHARTER

The cornerstone of international law concerning the maintenance of international peace and security is the UN Charter, which stipulates, inter alia, that:

- all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations (Article 2.4);
- the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security (Article 39);
- the Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures (Article 41);
- should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security (Article 42); and
- nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security (Article 51).

It is widely acknowledged by international law specialists that these rules establish a universal mechanism for maintaining international peace and security. However, now that ICTs are being developed or applied as a means of destruction (so-called "information weapons") and the international community has yet to arrive at a shared understanding concerning the place of information security within existing international law, the Charter could be interpreted in such a way as to provide international actors with a considerable degree of freedom to use ICTs to undertake aggressive actions and solve international disputes and conflicts.¹⁶

This strange set of circumstances stems from the fact that hostile actions in the information area have yet to be considered explicitly within international law on a par with hostile actions undertaken with traditional weaponry—even though the interconnectivity and dependence of today's world on ICTs mean that such an attack would be as devastating as a conventional attack—or perhaps even more so. Difficulties are further compounded by the lack of generally accepted interpretations as they apply to information security of such notions as "act of aggression" (Article 1), "force" (Article 2.4) and "armed attack" (Article 51).

INFORMATION ATTACKS AS AN ACT OF AGGRESSION

General Assembly resolution 3314 (XXIX) of 14 December 1974 defines an act of aggression.¹⁷ Article 3 of the Annex to the resolution states:

Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression:

- (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof,
- (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
- (c) The blockade of the ports or coasts of a State by the armed forces of another State;
- (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
- (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
- (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
- (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

Although this resolution was not adopted by consensus, its "soft law" provisions provide the UN Security Council and all members of the international community with a benchmark for recognizing acts of aggression.

The use of an information weapon could be interpreted as an act of aggression if the victimized state has grounds for believing that the attack was conducted by the armed forces of another state and was aimed at disrupting the functioning of military facilities, destroying defensive and economic capacity or violating the state's sovereignty over a particular territory.

THE ISSUE OF TERRITORY

In accordance with Article 41 of the UN Charter, among the measures available to the Security Council to give effect to its decisions include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication", i.e. a blockade. However, traditionally a blockade is imposed along the external borders of a state, while today an information blockade could cross into the territory of a state, affecting every house, office, institution or business.

A cyber-blockade may be seen as interference in the internal affairs of a state, a violation of its sovereignty, or even a partial seizure of its national territory—actions which violate the international norm under consideration. This rule degenerates into farce if measures to impose and maintain an "information blockade" are implemented by a state's armed forces. In such a case the attacked state

could invoke its inherent right of individual or collective self-defence, which implies the use of military force and conventional weapons.

Thus, 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, as recent events have shown.

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."¹⁸ 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."¹⁹ 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.

PERFIDY

In relation to information warfare, the problem of preventing perfidy is one of the most urgent in international humanitarian law.

In accordance with Article 23 of the Hague Convention, belligerents are forbidden "to kill or wound treacherously individuals belonging to the hostile nation or army". Thus the spirit of chivalry

should persist in relations between belligerents even during hostilities. The prohibition of killing or wounding the enemy in violation of this promise is the essence of this legal norm.

It would be reasonable to apply the same requirement to the behaviour of the parties to an inter-state conflict who launch ICT attacks on the civilian information infrastructure of another state. Commercial software and hardware used at infrastructure facilities are purchased with a certain guarantee of quality and security. An information attack would be facilitated if there were prepared "positions" in the software of ICT systems of the opposing party. These positions, for example, could be programs embedded in the software without the buyer's knowledge or consent. The incorporation of, for instance, malicious sleeping code or "backdoors" into such products is a deliberate breach of faith and a calculated violation of trust, and could be considered a form of perfidious behaviour. Acts of perfidy are already outlawed under international humanitarian law.²⁰

Concluding suggestions

In conclusion, the international community has several areas to develop which would ultimately strengthen international information security. In the legal area, these include:

- determining the legality of the hostile use of ICTs;
- determining norms regulating operation, support and usage of the global information infrastructure;
- consolidating technical regulations in the field of information security and investigative procedures for identifying the perpetrator of an information attack;
- forbidding the use of ICTs to damage critical infrastructure facilities;
- establishing a system of "cyber identification" for critical infrastructure facilities;
- updating the belligerents' rules of behaviour to take into account the global information infrastructure and its infrastructural elements situated in neutral states;
- developing confidence measures in relation to commercially available software; and
- extending the prohibition of perfidy to commercial ICT products.

Notes

1. Deirdre Collings and Rafal Rohozinski, *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations* (Workshop Report), United States Army War College 2006, p. 10.
2. *Военный энциклопедический словарь* [Military Encyclopedia], 1983, Moscow, Военное издательство, p. 523.
3. Signed in Moscow, 2 September 1998.
4. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/53/70, 4 January 1999.
5. General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General*, UN document A/54/213, 10 August 1999.
6. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/54/49, 23 December 1999.
7. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/56/19, 7 January 2002.
8. Ibid.
9. This contribution, entitled "Issues Connected with the Work of the Group of Governmental Experts on Information Security", is contained within General Assembly, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General*, UN document A/58/373, 17 September 2003, page 9.
10. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/61/54, 19 December 2006.

11. See for example, General Assembly, Creation of a Global Culture of Cybersecurity, UN document A/RES/57/239, 31 January 2003; and General Assembly, Creation of a Global Culture of Cybersecurity and the protection of critical information infrastructures, UN document A/RES/58/199, 30 January 2004.
12. This section is based on the contribution of the Russian Federation to the Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security. See General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General, Addendum*, UN document A/56/164/Add.1, 3 October 2001.
13. *Ibid.*, Section 3, page 3.
14. See, for example, the 2006 statement of Secretary of the Air Force Michael W. Wynne, *Cyberspace as a Domain in which the Air Force Flies and Fights*, at <www.af.mil/library/speeches/speech.asp?id=283>.
15. Karin Bystrom (ed.), *Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, 17–19 November 2004, Stockholm, 2005.
16. Thomas C. Wingfield, *The Law of Information Conflict. National Security Law in Cyberspace*, Aegis Research Corporation, 2000.
17. General Assembly, Definition of Aggression, Resolution 3314 (XXIX), 14 December 1974.
18. Laws and Customs of War on Land (Hague IV), 18 October 1907, Article 25.
19. *Ibid.*, Article 27.
20. Additional Protocol I of the Geneva Conventions, Article 37.

