United Nations A/56/164/Add.1

General Assembly

Distr.: General
3 October 2001
English
Original: Russian

Fifty-sixth session
Agenda item 69
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Addendum

Contents

01-56157 (E) 121001 121001

II. Replies received from Governments

Russian Federation

[Original: Russian]
[21 June 2001]

General appreciation of the issues of information security

Threats to international information security

In paragraph 1 of its resolution 55/28, the General Assembly calls on Member States to promote the consideration of existing and potential threats in the field of information security. In the draft proposal by the Russian Federation, entitled "Principles of international information security" (cf. A/55/140, chap. II), threats to information security are defined as factors that endanger the basic interests of the individual, of society and of the State in the information area.

In the view of the Russian Federation, these threats include:

1. **Development, creation and use of means of influencing or damaging another State's information resources and telecommunications systems**

– Electronic or psychoelectronic means used by illegal (unconstitutional) armed organizations, terrorist groups or individuals for the temporary or permanent neutralization of electronic installations or systems.

– Means of influencing the programme resources of electronic control modules for the purpose of destroying them or altering their operational algorithm.

– Means of influencing the information communication process for the purpose of halting or disrupting it through interference with the signal distribution environment and the functioning of the algorithm.

– Means of spreading disinformation or creating in the information area a virtual picture partially or totally misrepresenting reality.

– Means of acting on the human mind and the subconscious to produce disorientation, loss of will power or temporary destabilization.

2. **Deliberate use of information to influence another State's vital structures**

The information weapon is particularly dangerous when used against military and civilian buildings and State systems and institutions, the disruption of the normal functioning of which constitutes a direct threat to national security.

Unauthorized penetration, for example into computerized power control systems, could bring about a total paralysis of a country's life support infrastructure and, if nuclear power stations are involved, cause a catastrophic result comparable to the Chernobyl tragedy.

Criminal or terrorist associations obtaining unauthorized access to information concerning scientific and technical defence-related or dual-purpose studies could use it to produce the most advanced types of weapon for their own criminal purposes or for political blackmail.

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

Influencing information resources in the area of credit and finance, for example by 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 total economic collapse and, inevitably, cause serious complications in its international relations.

Massive destruction of the telecommunications infrastructure through the use of information weapons

amounts to an attack on State control and decision-making systems.

Hostile use of information to attack anti-aircraft, anti-missile and other defence communication and control systems leaves a State defenceless before a potential aggressor and deprives it of the possibility of exercising its legitimate right of self-defence.

Deliberate disorganization of the production process could also have a disastrous effect on enterprises posing heightened technological or environmental risks in the chemical, biological and fuel industries.

Disorganization of the communication, control and transportation systems of services dedicated to saving lives and dealing with natural disasters or other emergency situations could often increase the loss of life and property in such situations.

3. Use of information with a view to undermining other States' economic and social systems and psychological manipulation of a population for the purpose of destabilizing society

The deliberate use of information to damage an opponent or a competitor is hardly a new invention. Today, however, owing to the widespread use of modern telecommunication technologies and the formation of global information networks, the potential for such misuse has greatly increased. The opportunities for carrying out massive or total information attacks mean that, rather than being of an auxiliary nature, information weapons become a basic instrument of combat.

At the same time, the field of information is becoming a principal defining factor in the life of every society and actively impinges on virtually every aspect of State security. As progress is made in information technology, this influence will grow. 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.

4. Unsanctioned interference in information and telecommunications systems and information resources and their illegal use

Practically every modern Government encounters or may encounter unsanctioned interference in its information systems; indeed, there is a clear trend towards an increase in such activity. The danger of such interference is that it may set off a chain reaction of dangerous consequences: the experience of hackers may be used by criminal groups and their "achievements" may in turn be used as a weapon to carry out hostile, or even military, actions at the inter-State level.

Moreover, modern conditions of social and economic development exacerbate the contradictions between society's requirements for wider access to and free exchange of information, on the one hand, and the obvious need to maintain restrictions on such access and exchange, on the other.

At the same time, although each country may define in its laws and regulations what it means by unsanctioned interference in information systems or their illegal use, this varies widely from country to country, ranging from a minor administrative infringement to a criminal offence. Many countries have not determined their attitude to such activities at all.

It is thus possible for a lawbreaker to operate on international information system channels from his home territory, staying fully within his own national legislation, and yet remain outside the jurisdiction of the State with respect to which he has actually broken the law.

One way out might be to improve technological protection for information networks, but only for States which possess the requisite technical — and, above all, financial — resources.

Logically, such a situation points to the necessity of harmonizing existing national legislation and establishing a universal, international legal basis of accountability for such crimes and offences.

5. Actions to dominate and control the information area

The globalization process is characterized, in relation to the information area, by such features as a higher degree of standardization, which facilitates access by countries having a developed economic and information structure to the telecommunication markets of developing States. The less developed countries have no choice but to accept these standards and permit the use of the new technologies in their information area. Given the liberalization of the information technology market and free information exchange, they find themselves in the dominant information field of other States, with results that may be detrimental to their national security.

6. Preventing access to the most recent information technologies and creating a situation in which other States are technologically dependent in the information sphere

The reasons for preventing or restricting access by other countries to the most recent information technologies are similar to those relating to any other form of high technology. A restriction may, on the one hand, be imposed out of purely economic considerations, a desire to monopolize a given aspect of the market, or else it may have a political origin, such as sanctions, actions in response to "unfriendly" countries or national security considerations. Either way, there may well exist a desire to maintain or create a situation in which some States are technologically dependent on others in the field of information.

In any case, the fact is that in the twenty-first century information technologies have assumed critical importance for all States, which must have access to them in order to survive.

It should be borne in mind that a crucial factor in the creation of an information weapon is that the applicable information technologies will generally be found initially in the civilian sector and may only later be transferred to the military sector.

In view of all these factors, the question of restricted access to information technologies should obviously arise only in the context of the prevention of their use as weapons or as a tool in the production of new types of destructive weapon, or else for illegal purposes or for purposes detrimental to general security. Any other reasons for placing restrictive conditions on any future international information security regime should be considered unacceptable.

7. Aiding action by international terrorist, extremist or criminal associations, organizations, groups or individual lawbreakers that pose a threat to a State's information resources and vital structures

The unprecedented development of corporate, State and international information systems and the simultaneous expansion of opportunities of access to them have attained such a level that today practically every member of the international community will be exposed to a real risk of electronic attack by criminals or terrorists. The likelihood of such a risk will, of course, increase in proportion to the development of the global infrastructure of such systems and will inevitably take on a transboundary dimension.

Crime and terrorism using information systems are both illegal activities, although they differ in their aims. A criminal using information systems acts for purely mercenary or destructive reasons, while terrorists operate in cyberspace for the same purposes as political terrorism in general.

The means of carrying out such activities may include a variety of information weapons.

Using special computer programmes, techniques and technology, terrorists are able to:

- Destroy, distort or manipulate various aspects of the information infrastructure;
- Steal important information;
- Alter official and factual data for their own purposes;
- Take over or block channels of the mass media for the dissemination of disinformation, panic-mongering, threats of terrorist action or statements of their own demands;
- Disable communications systems by means of artificial overload;
- Disseminate threats of terrorist action in the information space, with serious political, economic, social or other dangerous consequences.

The tactics of information terrorism are that the terrorist act should have dangerous consequences, become widely known and be generally talked about. Unprotected information systems unfortunately offer ample opportunities for this.

8. Formulation and adoption by States of plans or doctrines providing for the possibility of waging information wars and capable of provoking an arms race and causing tension in relations among States, and of leading to information wars per se

One of the main elements of the defence strategy of many technologically advanced States today is to build up a mass of information which has military potential, both defensive and offensive. This strategy is enshrined in the corresponding national doctrines. In view of the growing role of information warfare and the means of information combat, there is greater scrutiny of traditional definitions of threats to national sovereignty, the observance of the principles and norms of international law, the nature of economic competition and the role of individual States in international affairs. Increasing attention is also being paid to strategic information warfare, which is a wholly new form of conflict.

The combination of economic and information power makes it possible to avoid traditional "harsh" forms of coercion using military force, yet be just as effective in influencing the development of a given international political situation.

The reasoning behind these new strategies is as follows:

– The development of information technologies does not prompt such a sharply negative reaction among other countries as a constant build-up of conventional weapons or, even more, weapons of mass destruction;

– The emphasis on developing information systems is attractive, because such systems correspond more closely to the concept of dual-purpose technologies and in many cases may have both military and civilian commercial uses;

– A State which is a leader in the development and application of information technologies reinforces its monopoly on the acquisition of strategic information and is thus able to react all the more effectively at times of international tension.

Another factor is that the use of information weapons can significantly reduce losses and damage in comparison with "traditional" military action. That is obviously why efforts are made to convey the impression that information operations are "humane".

On the other hand, every State can obviously see the advantages and the risks connected with the development of information technologies and will make every effort to react adequately to a changed situation. The future development of plans and doctrines for information warfare may well lead to a significant increase in the number of countries in possession of an arsenal of information weapons and thus to the start of an arms race at a new technical level. The weapons control situation could ultimately return to the state of affairs characteristic of the cold war period.

9. Use of information technologies and means to the detriment of basic human rights and freedoms in the field of information

The individual's interests in the field of information lie in the use of his or her right and freedom of access to information for the purposes of lawful activity or spiritual or intellectual development, in the maintenance of personal and family privacy, private correspondence and other electronic communications and in the protection of personal honour and dignity.

The development and widespread use of the most recent information technologies and means are currently creating unprecedented opportunities for realizing the right to information. The growth in the use of information technologies in everyday life and the development of information networks has the corollary, however, that ever more information concerning the private lives of individuals is becoming available on open databases. At the same time, there is a danger of unlawful restrictions by the authorities on access by individuals to the open information resources provided by federal bodies, local authority bodies, archives or any other open, socially significant information.

Any future international information security regime should provide for a harmonized ban on the collection, storage, use or dissemination of information

about a person's private life without his or her agreement and on restrictions to public access to information, except where sanctioned in law.

10. Transboundary dissemination of information, in contravention of the principles and norms of international law and the domestic legislation of specific countries

The globalization of the information area has blurred the traditional concepts of geographical, State and administrative boundaries or areas of jurisdiction that normally delimit national security. That being so, the need arises to define clearly where risks may arise, whether internally or externally. For example, a hostile military information operation against another State could be disguised as the action of "local" criminals. In other words, States that were previously in a position to ensure a legal regime of information exchange at their own internal level find themselves defenceless, in the new situation, against the transmission from abroad to their territory of information which may be unlawful or destructive, including pornography, disinformation, information indicative of racial discrimination or intolerance, information aimed at inciting social, national or religious hatred, information of a subversive nature or information emanating from and serving the interests of international criminal and terrorist groups.

11. Manipulation of information flows, disinformation and concealment of information with a view to undermining a society's psychological and spiritual environment and eroding traditional cultural, moral, ethical and aesthetic values

The workings of the information environment and information activities can substantially alter public perceptions and the behaviour of large groups in society. A particular risk is presented by such forms of influence as manipulation — a kind of psychological pressure which, when exerted, arouses in an individual or social group feelings that do not correspond with reality. An unstable, tense political situation increases the effectiveness of such manipulation. Feeding widespread disinformation into the system or else concealing true information in such a situation makes the objective assessment of events and contributory factors impossible. Public opinion is particularly open to such influences.

Backed up by all the power available to the modern information structure, such actions can lead to the destruction of a society's psychological environment and its cultural and other spiritual values, creating a war of cultures. The demoralization of society then creates the conditions for obliterating that nation's self-awareness and crushing its will to resist potential aggression.