

Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law

Sergei KOMOV, Sergei KOROTKOV and Igor DYLEVSKI

Nearly a decade has passed since the Russian Federation launched its initiative within the United Nations to address the issue of international information security (IIS). This complex issue is closely related to a number of fundamental principles of international law, including the prohibition of wars of aggression, the non-use of force or threat of force, and non-interference in another state's internal affairs.

The shocks suffered by mankind as a result of two World Wars played a special role in the international community's transition to civilized means of resolving international problems. Following the First World War, the term "war of aggression" was referred to as an international crime for the first time in a number of international instruments. The Kellogg-Briand Pact was the first multilateral treaty to set forth in international law the principle prohibiting wars of aggression.¹ The treaty proclaimed that war should be renounced as an instrument of national policy to settle international disputes and that all disputes should be settled peacefully.

After the Second World War, the prohibition on wars of aggression further evolved into a comprehensive principle of the non-use of force or threat of force in international relations. The principle of non-interference in the internal affairs of other states has also developed as an imperative principle of international law.

The Soviet Union played a pivotal role in establishing the principle of prohibition of wars of aggression and its successive transformation into the principles of non-use of force and non-threat of force. In particular, in 1933 the Soviet Union tabled a draft definition of aggression at the General Commission of the International Conference on Disarmament; although this definition was not adopted, it laid the foundation for many international instruments developed following the Second World War. In 1953, the Soviet delegation submitted a new draft definition of aggression to the Special Committee established by the UN General Assembly.²

In hindsight, an important advantage of the 1953 draft definition was its comprehensive nature, addressing four major types of aggression: direct (military), indirect, economic and ideological.³ In particular, it proposed to recognize that a state had committed indirect aggression if it was the first to:

- a) encourage subversive activities against another state (through terrorist attack, diversion, etc.);
- b) contribute to inciting civil war in the other state; or
- c) contribute to a coup d'état in another state or a policy change that would favour an aggressor.

Sergei Komov, Sergei Korotkov and Igor Dylevski are experts at the Ministry of Defence of the Russian Federation. They took part in the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2004–2005) and the relevant Group of Experts of the Shanghai Cooperation Organization Member Countries (2006–2007).

The following were considered as acts of ideological aggression:

- a) encouraging war propaganda;
- b) encouraging propaganda promoting the use of nuclear, bacteriological, chemical and other weapons of mass destruction; and
- c) supporting propaganda of Fascist or Nazi ideas of race and national exclusiveness, hate and depreciation towards other nations.

The draft definition also specified that the acts of aggression listed were not exhaustive, and that the UN Security Council could also consider other acts as aggression.

As a result of significant differences among the members of the Special Committee at its VII session, a draft definition of aggression was ultimately agreed upon that included only the military component. In December 1974, this definition was adopted by the UN General Assembly.⁴ That resolution sets forth a general definition of aggression (Article 1), specifies the main prima facie evidence of an act of aggression (Article 2) and lists major acts of aggression (Article 3). It also stresses that the list is not exhaustive and that the Security Council may determine that other acts constitute aggression under the provisions of the Charter (Article 4). In addition, it stipulates that "no consideration of whatever nature, whether political, economic, military or otherwise, may serve as a justification for aggression" (Article 5).

A cornerstone in the transformation of the principle concerning prohibition of wars of aggression into a more fundamental principle of non-use of force or threat of force was the UN Charter, which states 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).

Other international instruments confirmed and further developed this principle, turning it into an imperative norm of international law. In particular, the 1970 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations⁵ states that:

A war of aggression constitutes a crime against the peace, for which there is responsibility under international law.

In accordance with the purposes and principles of the United Nations, States have the duty to refrain from propaganda for wars of aggression.

...

Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of their right to self-determination and freedom and independence.⁶

Moreover, in this declaration the principle of non-use of force or threat of force is connected with the principle of non-intervention in the internal affairs of another state, affirming that:

... armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.

No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed

towards the violent overthrow of the régime of another State, or interfere in civil strife in another State.

The use of force to deprive peoples of their national identity constitutes a violation of their inalienable rights and of the principle of non-intervention.⁷

On the threshold of the third millennium many experts came to understand the necessity of legally prohibiting the use not only of the force of arms, but also of any other violence that constitutes an unlawful use of force for the purpose of aggression or intervention in the internal affairs of another state. Such a broad interpretation of the notion of "force" covers both economic and energy coercion, as well as other forms of violence in international relations.

Today, all societies are information dependent. The conduct of so-called "information operations" is therefore one of the potentially most damaging forms of force. These operations primarily aim at disrupting the functioning of the enemy's key military, industrial and administrative facilities and critical systems, and at manipulating information and exerting psychological influences on another state's political and military authorities, troops and civil population using, in the first place, information and communication technologies (ICTs).

ICTs make it possible to carry out electronic and computer attacks that are fundamentally different from traditional physical attacks. The use of electronic means takes warfare from the physical dimension to the virtual one. Today, a state can be attacked without its territory ever being physically invaded. The damage from such an attack may take different forms, for instance, technical failure of critical industrial, economic, energy and transport facilities, as well as financial collapse and large-scale crisis. Additionally, significant non-material damage could be inflicted as a result of disruption of civil order and military authority, including demoralization or disorientation of the population or mass panic.

Today, a state can be attacked without its territory ever being physically invaded.

The United States is considered to be the world leader in information operations, and intends to continue increasing its already existing powerful intelligence resources, and electronic warfare and psychological operations capacities.⁸ For example, the US Air Force has announced the creation the Air Force Cyber Command, which will become operational this year. Within the US Strategic Command (STRATCOM), the Joint Functional Component Command for Network Warfare is the leading unit for information operations.⁹

The potential of information operations is evident to military experts. However, information operations are a relatively new phenomenon in international relations. For numerous general and political reasons, members of the international community have yet to undertake a proper international legal evaluation of the issue.

It comes as no surprise that the United States is averse to attempts to discuss military aspects of the problem of international information security. A key participant in most major military actions of the past fifty years, it traditionally does not recognize some important, generally accepted provisions regulating the use of force in international relations and intervention in the internal affairs of other states. This is not a new development: as early as the mid-twentieth century during the discussion of the ideological component of the Soviet definition of the notion "aggression" an American representative voiced disagreement, stating that what may be considered propaganda in one country may be just the statement of a free press in another.¹⁰ More recently, in the context of developing the Rome Statute of the International Criminal Court, the US delegation raised an objection to the 1974 definition of aggression, an action which some have interpreted as hedging against the possibility that aggression be considered—and thus responsibility for such—an international crime.¹¹

For reasons such as these, in 2005 the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security¹² was unable to reach consensus on the adoption of its final substantive report. Thus, the opportunity to comprehensively address the problem of IIS in an international expert-level forum was postponed until 2009, when a new Group of Governmental Experts is scheduled to begin work.

As to the legal aspect of the problem, the way forward is, first of all, the application of universally accepted principles of international law in inter-state relations to the field of planning and execution of information operations. This will naturally require the adaptation of these principles to the specific character of these new inter-state relations. This approach will lay the necessary international legal foundation for addressing both the problem of ensuring IIS in general, and its political and military aspects in particular. Legal aspects of other relevant fields, such as outer space law, humanitarian law, and international legal responsibility, will also need to be taken into consideration.

The application and development of key principles of international law

At present international law lacks provisions that unambiguously prohibit, allow or otherwise regulate information operations. However, such issues could be considered in the context of the application of key international legal principles. In particular, the aforementioned 1974 definition of aggression¹³ states that not only military violence but also other acts of aggression as defined by the Security Council qualify as aggression under the UN Charter. However, this provision has yet to be utilized. Even earlier, in 1953 Iran proposed in the General Assembly that any action that indisputably serves the purpose of an armed attack or results in coercion prejudicing the independence of a state should be recognized as aggression.

Since the adoption of the UN Charter the principle of non-use of force or threat of force against the territorial integrity or political independence of another state has been applied only in its physical sense. The 1973 oil embargo led many nations to question the point of view that use of force did not include economic coercive measures, as the UN Charter prohibits the threat of force and its use in any way that is incompatible with the Purposes of the United Nations. Other states insisted that the said provision did not apply to such a manifestation of force.¹⁴

Ultimately, United Nations resolutions and enforcement practice do not provide a definitive answer to the question of whether an attack as part of an information campaign would be classified as aggression, use of force or threat of force. Therefore, there is a need to develop these principles to define in more detail the concepts of "aggression", "force" and "threat of force" in relation to IIS.

As for classifying "information and psychological influence" as intervention in the domestic affairs of a state, this issue could be resolved on the basis of the provisions of the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations¹⁵ and the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty,¹⁶ the latter of which states that "No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned."¹⁷

Although these documents do not provide a clear definition of "intervention in the domestic affairs of states", they contain an open-ended list of actions that qualify as intervention. This legal platform leads us to the conclusion that almost any information operation with a psychological bias, implemented in peacetime with respect to another state, would qualify as intervention in its domestic affairs. Even good intentions, such as the advancement of democracy, **cannot** justify such operations.

The 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States further developed the principle of non-intervention in the domestic affairs of states. These rights and obligations of states include:

- "The right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, *inter alia*, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order";¹⁸
- "The duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States";¹⁹ and
- "The right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, co-operation and friendly relations among States and nations".²⁰

Consequently, the dissemination of disinformation by one state against another, widely used in information operations, may be considered intervention in its domestic affairs and should entail corresponding measures of international responsibility.

International law prohibits the violation of a neutral state's territory by a belligerent's armed forces. However, belligerent states are not under obligation to refrain from using open computer networks of a neutral state. Moreover, the use of computer networks crossing the territory of a neutral state to conduct information operations could be considered as a violation of its territory. These forms of aggression can therefore be considered illegitimate acts of warfare against a neutral state. On the other hand, if a neutral state refuses to oppose the use of its networks for attacking another party, it might be targeted by the state against which an information operation is being conducted under the pretext that its networks were used.

The legality of retaliatory actions against information operations is another significant legal issue. To clarify this issue, the international community has to resolve a number of integrated problems. In particular, it is necessary to be able to identify with certainty the source of a cyber attack and to consider the issue of territorial jurisdiction.

According to international law, foreign agents cannot carry out their activities within the territory of another state without its permission. The UN International Court of Justice in the Corfu Channel Case (1949) ruled that the entry of the British Royal Navy into Albanian territorial waters without permission was seen as a manifestation of force and a violation of international law.²¹ More recently, the Council of Europe has attempted to find a solution based on international law to the territorial jurisdiction issue with a view to ensuring international information security in computer networks.²² Some experts believe that this has not been a very successful approach, believing that it entails the violation of such principles as national sovereignty and non-interference in the internal affairs of other states.

In accordance with Article 51 of the UN Charter, individual or collective self-defence against armed aggression is regarded as lawful use of force. At the same time it is not clear whether this article permits retaliatory military action against a state carrying out an information operation. In the 1986 case Nicaragua against the United States of America, the UN International Court of Justice found that states are not entitled to take military action in retaliation for acts that do not constitute military aggression.²³ Based upon this precedent, unless cyber attacks are qualified as armed aggression, the injured party will not have the legal right to respond in self-defence using conventional weapons. Yet ironically, within the current legal ambiguity surrounding IIS issues, symmetrical retaliatory measures (i.e. information attacks) could be taken with impunity. The simple legal solution to this problem

requires requesting the Security Council to qualify a cyber attack as posing a threat to the peace or as an act of aggression, which would then permit an attacked state to take certain measures provided for within UN Charter.

Contemporary international law has a number of concepts to describe actions taken by one state against another as aggression, use of force or threat of force and interference in internal affairs. All of these concepts apply to both armed forces and state-backed terrorist groups. Today's interpretation of these concepts is conditioned by the historical practice of waging warfare with conventional military means. This makes it very hard to define the term "information operations" carried out by either traditional or fundamentally new means. It is easiest to qualify the concept of "interference in the internal affairs of a state", which comprises all possible means that have information and psychological effects. As to such information effects as electronic and cyber attacks, we think that it is advisable they are included within the concepts of "aggression", as well as the "use of force" or "threat of force". Moreover, a mechanism in international law already exists, via the UN Security Council, to determine a threat to the peace or an act of aggression. It is this mechanism used under the UN Charter that must establish whether an information operation has occurred and which state conducted it, as well as to determine appropriate steps to restore international peace and security and appropriate measures to prevent the further violation of these principles.

Application and development of principles in select branches of international law

Important provisions concerning the military aspects of information security are contained in documents that form the basis of such branches of international law as international telecommunications law, space law, international humanitarian law, law of international legal responsibility of states, and others.

Some actions taken as part of information operations related to electronic warfare may be covered by instruments of international telecommunications law. Thus, under the Constitution of the International Telecommunication Union (ITU), all communication stations, whatever their purpose (including military ones), must be established and operated in such a manner so as not to cause harmful interference to the radio services or communications of other Member States. Member States further agree to take the steps required to prevent the transmission or circulation of false or deceptive distress, urgency, safety or identification signals, and to collaborate in locating and identifying stations under their jurisdiction transmitting such signals.²⁴

Activities carried out as part of peacetime information operations entailing consequences prohibited by the ITU Constitution may therefore be considered as violating this international agreement. However, there would be no violation if the information operation is qualified as an armed conflict or if it occurred during an armed conflict.

If satellites were to be used to conduct an information operation, *international space law* may apply. The cornerstone of international space law, the Outer Space Treaty, obliges states to carry out their space activities exclusively for peaceful purposes.²⁵ However, some believe that space law does not directly prohibit the use of satellites for conducting information operations. Within the Conference on Disarmament, the United States has opposed discussion of the 2002 working paper "Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects".²⁶ In the General Assembly, it has voted against resolutions on the Prevention of an Arms Race in Outer Space²⁷ and on Transparency and Confidence-Building Measures in Outer Space Activities,²⁸ stating in its Explanation of Vote that there is no arms race in outer space and "thus no arms control problem for the international community to address." Some fear that this position aims to maintain conditions allowing the use of outer space for conducting global information operations.

An essential principle of international humanitarian law (IHL) is that of humanity in armed struggle, which prohibits the use of force unless it is justified by military necessity. The principle of humanity concerns methods and means of warfare, as well as protection of victims of war. Through IHL, belligerents are limited in their means of damaging the enemy. For example, it is prohibited to employ weapons of indiscriminate effect (i.e. directed both at military objectives and civilian objects) or causing superfluous injury or unnecessary suffering.²⁹ Hence, to avoid indiscriminate effects, hostilities—including in the form of information operations—should be limited to military objectives, i.e. to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

During times of conflict, protection of civilian objects, including against information operations, should be ensured in two ways:

- special precautionary measures should be taken to verify that the objective to be attacked is a military one. To avoid incidental damage to civilian objects, it is important to refrain from any attack against civilian objects which may be expected to cause damage excessive in relation to the concrete military advantage anticipated;
- special protection of objects indispensable to the survival of the civilian population, works and installations that would pose great threat if damaged or destroyed (such as nuclear power plants, dams and dykes), cultural objects and those related to civil defence.

In one view, the best way to define information operations in relation to IHL is on the basis of the scale and gravity of their consequences.³⁰ Disorganization of the financial system of a state, man-made disasters and panic entailed by information operations may cause mass casualties among civilians. Additionally, the dual-use nature of ICTs has eliminated the distinction between many military and civilian ICT systems. In addition to military gains, information operations may therefore lead to malfunction of civilian objects. Hence, under IHL, information operations affecting such objects should be banned.

In one view, the best way to define information operations in relation to IHL is on the basis of the scale and gravity of their consequences.

International humanitarian law does not prohibit ruses of war, such as the use of camouflage, mock operations, misinformation, etc. At the same time, perfidy is prohibited. This includes: unlawful use of flag of truce, military emblems and uniform of the enemy, the United Nations and the Red Cross; or killing or capturing an adversary by resort to perfidy. However, it is very difficult to distinguish between perfidy and ruses of war in an information operation meant to manipulate the perceptions of the civilian population or military and political leaders. As no clear criteria have yet been established in international law to deal with this issue, some claim that manipulation of perception does not violate IHL. However, it should be recalled that it was the manipulation and distortion of information that justified the unleashing of two world wars in the past century, and some claim that manipulation of intelligence data misled world public opinion to legitimize recent actions in Iraq.

Finally, it should be noted that if information operations as a form of military action are covered by the existing rules of IHL, then it necessitates application of all existing agreements on laws and customs of **war with regard to such operations**.

As for the *international legal responsibility of states* for internationally wrongful acts (in case of breach of an international obligation by a state), this is well established in contemporary international law, specifically regarding the threat or use of force.

Crimes against peace, war crimes and crimes against humanity were for the first time qualified as gravest international crimes under the charters of the international military tribunals at Nürnberg and Tokyo. A 1946 UN General Assembly resolution³¹ recognized the principles contained in the Charter

of the Nürnberg Tribunal as principles of international law, i.e. rules establishing the responsibility of states and criminal responsibility of individuals for the commission of international crimes. These principles are universally recognized.

We believe that the foundations for a state's liability for internationally wrongful acts in connection with information operations are as follows:

- dissemination of information prohibited by international law, including war propaganda and advocacy of the use of force, propaganda of violence, provocative information, etc.;
- dissemination of information specifically intended to produce psychological and/or ideological effects on the population or on certain individuals (false information, information fomenting religious discord and other enmity, etc.);
- cyber attacks on information systems of the state's critical infrastructure and attacks on other infrastructure, when such attacks result in substantial economic damage; and
- radio jamming, transmitting or propagating false or deceptive distress, emergency, safety or identification signals, etc.

Depending on the gravity of their consequences, such acts could be qualified as international crimes, i.e. the gravest of offences involving severe measures of international responsibility.

Given the danger of information operations, for example against critical infrastructure facilities, it seems possible in principle to raise the issue of controls on manufacturing and proliferation of means of information warfare, sometimes referred to by the umbrella term "information weapons". Imposing export controls on special-purpose technology might be a means of ensuring control of such weapons. However, some elements such as expertise and widely available technologies are currently not subject to export controls. Thus, in order to create a comprehensive international legal information weapons control system, we should draw on the experience of designing and enforcing regimes and procedures for control established by international law in relation to other types of weapons, while taking into account the specific characteristics of information weapons.

Conclusion

In the last century, when chemical, biological and, finally, nuclear weapons were created, we were unable to develop international instruments on nuclear disarmament and instruments prohibiting biological and chemical weapons were adopted only belatedly. As for nuclear weapons, the international community has yet to agree on their ban.

Today, a completely new military and political threat is emerging. The international community should not permit this situation to happen again with regard to measures to counter the threat of proliferation of information weapons and to suppress the unpunished conduct of information operations. To this end, the international community should, as a matter of priority, overcome its apathy toward continued regular violations of universally recognized principles of international law and then collectively build a reliable international legal barrier to the emerging threat of information aggression.

Notes

1. Treaty for Renunciation of War as an Instrument of National Policy, signed in Paris on 27 August 1928.
2. UN document A/AC.66/L.2/Rev.1, 14 September 1953.
3. K.A. Baginyan, "Агрессия – тягчайшее международное преступление. К вопросу об определении агрессии" [Aggression as a Major International Offence. On the Definition Aggression], *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.

4. General Assembly, Definition of Aggression, UN resolution 3314 (XXIX), 14 December 1974.
5. General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN resolution 2625 (XXV), 24 October 1970, annex.
6. General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN resolution 2625 (XXV), 24 October 1970, annex.
7. Ibid.
8. United States Department of Defense Directive (DODD) S-3600.1, Information Operations, October 2001; DOD Information Operations Roadmap, 30 October 2003; FM 3-13 Information Operations: Doctrine, Tactics, Techniques and Procedures, 28 November 2003, SS FM 100-6; Joint Pub 3-13 Information Operations, 13 February 2006.
9. "A Special Subdivision for Neutralizing Foreign Media Created in the USA", *NEWSru.com*, 23 November 2005.
10. K.A. Baginyan, "Багинян К.А. Агрессия – тягчайшее международное преступление. К вопросу об определении агрессии." [Aggression as a Major International Offence. On the Definition Aggression], *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.
11. V.A. Kartashkin (ed.), *Human Rights and Armed Conflicts*, Norma Infra, Moscow, 2001, p. 137.
12. Established in accordance with the decision of the 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.
13. General Assembly, Definition of Aggression, UN resolution 3314 (XXIX), 14 December 1974.
14. K.A. Baginyan, "Ягчайшее международное преступление. К вопросу об определении агрессии" [Aggression as a Major International Offence. On the Definition Aggression], *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.
15. General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN resolution 2625 (XXV), 24 October 1970, annex.
16. General Assembly, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UN resolution 2131 (XX), 21 December 1965.
17. Ibid., paragraph 1.
18. General Assembly, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, UN document A/RES/36/103, 9 December 1981, §(c).
19. Ibid., §II(j).
20. Ibid., §III(d).
21. The Corfu Channel Case. Consideration on the merits. Decision of April 9, 1949, ICJ Reports, 1949, pp. 34–35.
22. Convention on Cybercrime (ETS No. 185), signed in Budapest on 23 November 2001.
23. The case on military and paramilitary activities in and against Nicaragua (Nicaragua against the United States of America). Decision of 27 June 1986, ICJ Reports, 1986, paragraphs 195, 232.
24. The Constitution of the International Telecommunication Union (adopted in Geneva on 22 December 1992), Articles 45, 47, 48.
25. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (signed on 27 January 1967).
26. Permanent Representatives of China and the Russian Federation, *Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects*, Conference on Disarmament document CD/1679, 28 June 2002.
27. General Assembly, Prevention of an Arms Race in Outer Space, UN document A/RES/61/58, 3 January 2007.
28. General Assembly, Transparency and Confidence-Building Measures in Outer Space Activities, UN document A/RES/61/75, 18 December 2006.
29. Additional Protocol I to the Geneva Conventions (adopted on 12 August 1949), Article 35 paragraph 2, Article 52 paragraph 2, Article 57.
30. Кубышкин А.В., *Международно-правовые проблемы обеспечения информационной безопасности государства* [The International Legal Problem of Ensuring Information Security of a State], Doctoral Thesis, Moscow State Law Academy, 2002.
31. General Assembly, Affirmation of the Principles of International Law Recognized by the Charter of the Nürnberg Tribunal, UN resolution 95 (I), 11 December 1946.

