International Law and the Problem of International Information Security

A. Krutskikh, A. Streltsov

THE IMPACT of information and communication technologies (ICT) on all aspects of human life, society and the State cannot be overemphasized. Apart from the obvious benefits in terms of economic, social and cultural development, the enhancement of the role of ICT in the contemporary world inevitably brings new risks for international and national security. There is already real evidence that the damage from the use of ICT for purposes contrary to the Charter of the United Nations, as well as for criminal and terrorist purposes may be comparable to the most destructive weapons. The list of potential targets for information weapon attacks includes not only the information resources of the Internet, but also the critical infrastructures of States in the industry, transport and energy sectors. What's more, the scale and technological level of such destructive impact are steadily increasing.

All countries without exception acknowledge the severity of threats of a criminal, terrorist and military-political nature in the information space. The international community has been engaged in discussion on how to ensure international information security (IIS) for more than a decade and a half. At this point, the apparent key problem is the lack of a full-fledged international legal framework governing ICT-related activities by States, including their military aspects.

The UN Group of Governmental Experts (GGE) on IIS set up in 2014 in accordance with Russia's resolution on the Developments in the Field of Information and Telecommunications in the Context of International Security, adopted by consensus at the 68th session of the UN General Assembly, is designated to study these issues. Russia has sponsored the

Andrey Krutskikh, Professor, Ambassador-at-Large, Ministry of Foreign Affairs of the Russian Federation, Doctor of Science (History)

Anatoly Streltsov, Professor, Deputy Director, Information Security Institute, Lomonosov Moscow State University, Doctor of Science (History), Doctor of Science (Technology), Doctor of Science (Law)

document for a number of years. Our resolution has always received consensus support, with more and more countries joining the list of its cosponsors every year (over 40 States in 2014.)

The UN GGE on IIS will convene for the fourth time.[1] In 2010 Russia's Chairmanship ended with the adoption of a report whose wording made it possible to lay the basis for a substantive discussion on IIS. As evaluated by Deborah Stokes, an Australian expert who headed the GGE in 2012-2013, the report "paved the way" for discussion of the most topical problems in this area, including the politico-military aspects of the use of ICT.[2]

Can we consider unauthorized access to the e-mail of a state leader or top-ranking official as interference in the internal affairs of a state?

The Australian Chairmanship, in turn, resulted in a document that consolidated the general interest of States in the peaceful use of ICT. In addition, the report of this GGE reached consensus on another fundamental issue, that of the applicability of international law to the use of ICT. The document lays out a balanced formula: while international law is generally applicable to the field, there has to be a common understanding as to the way States can apply it, and in what direction, if necessary, it should be adapted.

Obviously, not all legal norms relating to the traditional environments of human activity can "automatically" extend to cyberspace. At the international level, criteria for applying and adapting international law to interstate relations in the field of ICT use are still lacking. As the international community does not have a common understanding of the issues at stake, this hinders efforts to prevent conflict arising from the use of ICT; it also hinders work to demilitarize cyberspace.

The mandate of the new GGE, established in 2014, involves the study of existing and potential threats in the sphere of information security as well as possible cooperative measures to address them. They include norms, rules or principles of responsible behavior of States, confidence-building measures, discussion of ICTs in conflict and of how international law applies to the use of ICT by States. After four meetings, the Group is to formulate practical recommendations that should be the outcome of an international compromise.

This article offers a detailed overview of the issues arising from the application of international law to the digital environment. An active

debate on these issues is taking place in various international forums, particularly at the UN, reflecting attempts by States to find an international legal "panacea" against threats in the information space. The purpose of this article is not so much to suggest specific recipes, but to systematize the progress of international discussion.

1. How is unlawful use of ICTs interpreted within the present system of international legal norms?

International law has no reference to universally recognized notions of war or armed struggle. Moreover, there is no universally accepted definition of information war though some international acts include such definitions. There is also a need to study the attributes of information war and elaborate a universally recognized definition since some of the specifics of unlawful use of ICTs for the resolution of interstate differences are impeding in terms of its legal regulation:

- no "warhead situation" – it is impossible to trace the moment when the use of military force took place;
- transborder nature – the force can be applied aggressively by the unlawful use of ICTs against the adversary with no breach of its territorial borders;
- ICTs are not a weapon per se, which makes it difficult to classify an attack with the use of ICTs as an armed one.

Specific attributes of the ICTS are in compliance with the fact that any war waged to conquest or defeat the adversary violates the UN Charter and the principle of sovereign equality of states.

2. Can unlawful use of ICTs be classified as an aggression according to the UN GA Resolution 3314 "The Definition of Aggression" of 1974?

According to Article 2 of the document, state actions are qualified as aggression along with the criteria of the use of force, the first use of force, gravity and hostility regardless of whether the war has been declared or not. These provisions can be applied to information space though some norms of the document need to be adapted to the specific attributes of ICTs. Unlike the traditional interpretation of aggression, unlawful use of ICTs has no reference to the introduction of force or the traditional use of military force which impedes the classification of computer attacks as an act of aggression.

3. Does the term "weapon" apply to ICTs?

It is difficult to give an answer to this question as currently there are no international legal acts defining computer attacks as an armed attack. All the existing international legal principles such as "use of force," "act of aggression," "armed attack" take as a premise the weaponry and its utilization, particularly, the physical damage or seizure of territory.

The term "information weapon" is used in some international documents of the SCO and CIS,2 for example, in the annex to the Agreement on Cooperation of the CIS members in the field of information security (St. Petersburg, November 20, 2013): "Information weapon – information technologies, means and methods applied for the purpose of information war." The definition of "information war" is included into Article 1 of the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, June 16, 2009), which stipulates that the characteristics of information war include the impact on transportation, communication and air control systems, missile defense and other types of defense facilities as a result of which the State loses its defense capabilities in the face of an aggressor and fails to exercise its legitimate right to self-defense, breaching information infrastructure operation, which leads to the collapse of administrative and decision-making systems in the states, and computer attacks on critically important structures.

These approaches designed to define the key notions referring to unlawful use of ICTs for the purposes threatening international peace, security and stability can be used by international community as a basis for elaboration of a universally accepted definition of information weapon.

4. Which legal facts referring to unlawful use of ICTs can be qualified as the use of armed forces (within the meaning of Article 39 of the UN Charter) and enact the right to self-defense (within the meaning of Article 51 of the UN Charter)? How can the threshold level, which, if surpassed, qualifies the use of ICTs as an armed attack, be identified (within the meaning of Article 51 of the UN Charter)?

In case of unlawful use of ICTs physical damage is difficult to assess since losses are often intangible (for example, leaks of classified information on Wikileaks website). One of the tasks topping international

agenda is to identify the threshold level for the damage which, if surpassed, can qualify the use of ICTs as an aggression.

In this regard, the NATO decision to extend the collective defense principle (Article 5 of the Washington Treaty) to information space has to be specifically scrutinized. This decision, inter alia, runs counter to the NATO members' stance which rests on the assumption that there is no need to elaborate new treaties in the use of ICTs and that existing norms of international law can be applied "automatically."

5. Which legal facts referring to unlawful use of ICTs, including the one aimed at critical information infrastructure, can enact the right to self-defense (within the meaning of the Article 51 of the UN Charter) and how can they be objectified? Which international structures are in charge of legal assessment and objectification of legal facts?

In our view, Iran (or any other country in its position) cannot currently file a complaint to the International Court of Justice against one or a number of countries charging them with the Stuxnet attack on uranium enrichment centrifuges since, given the lack of international legal regulation in this field as well as relevant precedents, it's unclear what factual evidence is needed to carry out international justice and how to confirm its objectivity. These problems impede international justice in the field of IIS, inducing states to resort to non-legal reaction on computer attacks.

6. How can states' misuse be avoided in qualifying unlawful use of ICTs as a condition enacting the right to self-defense?

The exercise of the right to self-defense necessitates the elaboration of the criteria for the rationale and proportionality of the reaction.

7. Can national information infrastructure be regarded as a military object in case of a conflict stemming from unlawful use of ICTs? Can traditional weapons or ICTs designed to destroy such objects be used against this infrastructure?

8. Which information infrastructures have to be protected against unlawful use of ICTs for humanitarian considerations?

Assuming that international humanitarian law suggests the protection

of civilians and the objects critical in terms of their security (including critical information infrastructure), the norms of international humanitarian law have to be considerably adapted to the progress in the use of ICTs. Due consideration should be given to the fact that ICTs cannot be classified as objects in terms of international humanitarian law since ICTs is an umbrella term to define information processing by computation means, as well as the methods of its searching, collection, storage, processing and presentation.

9. How can the principles of proportionality and selectivity be observed in case of computer attacks? Do the limitations placed by international humanitarian law extend to certain types of information weapon (particularly, those referring to the use of weapons causing unnecessary suffering or have indiscriminate effects)?

10. How can states' misuse be avoided in defining subjects responsible for unlawful use of ICTs?

Qualification of unlawful use of ICTs as terrorist or criminal attack removes them from the sphere of international law and international humanitarian law and allows for unilateral retaliation which, in its turn, poses a threat to international peace and security.

11. Can the use of ICTs for the violation of social and political stability and public order of other state be classified as unlawful and be qualified as an interference into the internal affairs of a sovereign state (within the meaning of Article 2(4) of the UN Charter)?

12. How can a subject of unlawful use of ICTs be identified?

The anonymity of ICTs and, as a result, the difficulty of identifying aggressor can lead to attributing the fact of the use of force to the state whose information systems were used for unlawful purposes. As we see it, the use of the territory of the third state in this case forces it into the conflict with no responsibility for aggression attached.

13. How is the responsibility of a third state that allows for its information systems to be used for unlawful purposes identified?

We need to elaborate international legal norms enshrining state obligation not to allow for its national segment of information space to be used for computer attacks against third parties.

14. How can we identify the responsibility of a state for the actions of an actor authorized by this state to use ICTs for unlawful purposes?

According to the norms of international law, a state is responsible for the actions of its organs and persons acting under the state's control. But it can be difficult to determine whether the person acts in the interests of a state and under its control in information space.

15. How can the exercise of the state's right to neutrality be ensured when conflicting parties use its ICTs to violate international peace and security?

The main legal problem here is the exercise of the states' right to neutrality, when their information systems are used by third parties for computer attacks or other unlawful actions.

16. How can we distinguish between combatants and noncombatants in case of a conflict in information space, given anonymity of ICTs and their availability?

17. How can we identify the theater of war in information space?

18. How can we assess the relation between unlawful use of ICTs and the violation of state sovereignty? Can we consider unauthorized access to the e-mail of a state leader or top-ranking official as interference in the internal affairs of a state? Does this constitute a threat to international peace and security, act of aggression, and violation of a state sovereignty?

As we see it, unlawful use of ICTs falls under this classification only if it is a socially dangerous action inflicting serious consequences nationally and internationally.

19. Which international or national institutions are authorized to assess the threats arising from the unlawful use of ICTs for the purposes inconsistent with international peace and security as well as the conse-

quences for security of an individual state in terms of the violation of its sovereignty, territorial integrity and political independence? What criteria should these institutions be guided by?

Proceeding from the assumption that international legislation is enforced, in the first instance, by states, there is a concern that the consequences can be miscalculated posing a threat to international security.

20. What funds are supposed to be used to provide the states in need with the ICTs, software and technical means necessary to address unlawful use of ICTs for military, terrorist and criminal purposes? How can this be implemented? Which legal and technical acts are supposed to provide the basis for legislations of the states in need?

21. What efforts should be made to prevent the use of ICTs for terrorist and criminal purposes?

Nowadays, it seems difficult to accomplish because of the lack of the relevant legal framework. One of the attempts to establish multilateral effective mechanism in this sphere is the Council of Europe Convention on Cybercrime of 2001 (Budapest Convention). Russia, like many other countries, has not acceded to it since it deems unacceptable one of its key provisions on trans-border access to the data during the investigations. This provision contradicts the principle of state sovereignty. Article 32 stipulates that in the framework of mutual assistance there is a trans-border access capability without the authorization of another Party to publicly available (open source) stored computer data (paragraph "a") or to stored computer data if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data (paragraph "b"). However, provisions of the article are so vague that it is unclear who gives such permission, what resources it may concern and what powers this person has.

Russia has consistently voiced concerns that this article practically grants permission to penetrate into the networks of other state violating the principle of state sovereignty and contradicting the spirit of cooperation and respect between states. Moreover, the question arises, whether the Budapest Convention can be an attempt to legalize global espionage. Well-known disclosures by Edward Snowden made it clear that this issue is pressing.

Besides, rapid exploration of information space and the introduction of new technologies made the Budapest Convention out of date. During its development (1997-2001), many threats in the field of information security, including criminal offences, were unknown or considered insignificant. Since that new types of crimes, including the so-called bot-nets (computer networks which are infected by malicious software and allow committing illegal acts remotely) developed by hackers, have appeared. Besides, as an example, the Budapest Convention does not include references to anti-spam measures, "fishing," etc.

It is hard to combat new manifestations of terrorism in information space without its legal definition as well as criminalization of the concept of such terrorism and its components. The Budapest Convention does not cover such measures. Besides, the document provides for complex amendments procedure. Such amendments can be introduced only after its ratification by majority vote. Therefore, modification of the text of Convention is a complicated task.

A growing number of countries express solidarity with Russia that there is now a need to develop a UN Convention to combat cybercrime to exclude the most controversial provisions of the Budapest Universal Convention, draw on the positive experiences from it and at the same time guarantee sovereignty and non-interference in the internal affairs of States. A document of global reach is needed that takes into account the positions of all countries and is based on respect for the principle of State sovereignty.

22. How can the balance between security and freedom, the right to access to information and responsibility of states in information space be found?

According to the abovementioned UN GGE report, adopted in 2013, state efforts to ensure information security should be in harmony with the protection of human rights and fundamental freedoms. Espionage in information space, as well as attempts of a state to violate the right of users to privacy (unveiled by Snowden), pose a real threat to information security and bring to the fore the need to elaborate norms referring to the protection of human rights and data in information space. In this context, due attention should be paid to the International Covenant on Civil and Political Rights (1996) that enshrines right to freedom to seek, receive and disseminate information and ideas of all kinds, as well as special

duties and responsibilities subjected to certain restrictions, necessary for the respect of the rights or reputations of others or the protection of national security or of public order or of public health or morals.

23. How can the information exchange on critical information infrastructure and its protection be provided without making it an easy target?

Computer attacks on critical information infrastructure can leave thousands people with no water, food and electricity. The disruption of information systems managing the work of nuclear and hydro plants can cause high death toll. To maintain international peace and security, the responsibility of states to refrain from attacks on critical information infrastructure should be formalized. However, realization of this responsibility demands identification of such infrastructure, as well as the criteria for classification of particular objects of national or international critical infrastructure, which endangers such infrastructure, leaving it open to attack.

Thus, it is clear that the international community would take a long time to resolve this contradiction. However, it is also clear that time is running against us. The frequency of computer attacks has grown at a rate that far outpaces the progress of international negotiations on the subject. It seems that in parallel with the discussion of the whole range of problems related to critical infrastructure, use could be made of a "tactic of small steps" – for example, as an initial measure to protect the banking infrastructure and conclude a "non-aggression pact" for banks. In what ways could we have the relevant obligations of States formalized under international law? How could they be implemented in practice?

24. There is a problem of political and legal assessment of vulnerabilities found in the ICT products that can be used for unlawful purposes. The UN GGE 2013 Report notes the concern of the international community about the possibility of the inclusion in ICT of hidden malicious functions that can be used to damage national security, reduce the reliability of the use of ICT or erode confidence between the parties in the field of trade. Is there any way to guarantee that these vulnerabilities are not a built-in used to ensure information superiority in future? Which information on possible vulnerabilities of ICT products supplied to the market should states share if they seek to have transparent relations in this field? How can we regulate the order of information exchange on the vulnera-

bilities not covered by bilateral and multilateral treaties?

25. One of the fashionable themes actively promoted by the West at international venues is the so called "capacity building." Measures to overcome the "digital divide" between countries of varying technological advancement are both relevant and urgent, but how to exclude the possibility of their use for malicious purposes? Building digital capacities can be potentially threatening to security and sovereignty of states which are the recipients of international aid in this field. How can we ensure that a digital gap does not become a disguise for business lobbying? How can we build digital capacity without simultaneous expansion of the secret services capacity to access private data of the recipients, which will inevitably violate their national security?

26. To what extent does the present Internet governance model correspond to the interests of international and national information security? How should it be reformed taking into consideration a "multistakehoder" approach? Meanwhile donor countries will want greater security assurances. How to avoid the appearance of a digital Frankenstein and prevent the use of transferred technology against them themselves?

27. Given scientific and technological progress, how can the definition of ICTs be updated to embrace the developments in the sphere of robotic engineering, artificial intellect, etc.?

***

AS APTLY COMPARED by Katherine Getao, Kenya's representative at the UN GGE 2014/2015, ICTs are a "moving target," so dynamic that legal norms sometimes are lagging behind the new information reality. However, relations between nations must be governable by the principles of international law. Yet it is undeniable that many of its provisions stem from prior to the cyber revolution and mainly sought to provide governance for traditional international relations, without regard to the impact of the so-called virtual factor. New technological realities call for refining and upgrading international law, if not in spirit, then form.

There is a need to elaborate a specific terminology, including such definitions as "information weapons," "information warfare," "act of ICT-based aggression," etc. The principles of international humanitarian

law would undergo substantial adjustment. In some cases, new legal norms for international relations in information space should emerge. It is necessary to adapt the generally recognized principles and norms of international law to the specifics of digital space.

Russia proceeds from the assumption that the generally recognized principles of international law jus cogens, arising from the UN Charter, and relevant norms of international law, such as non-interference in the internal affairs of states and non-use of force and threat of force, would remain immutable in both physical and digital space.

According to the most frequently cited data in international media, nowadays approximately 130 states are working on information weapons. They adopt relevant doctrines and establish special units for information warfare. Furthermore, no line can be drawn between offensive and defensive potential in information space. Building capacities triggers the risks of their utilization and brings to the forefront the need to demilitarize information space and adopt relevant international legal obligations. Some NATO experts develop approaches to regulate information confrontation (such as *Tallinn Manual on the International Law Applicable to Cyber Warfare*). Russia follows a diametrically opposed policy of averting military and political confrontations in information space. It believes that the top priority is to anchor the rules of prevention of conflicts arising from the unlawful use of ICTs in international law.

Some of these rules are included into the Convention on International Information Security, a concept presented by Russia in Yekaterinburg (September 21-22, 2011) at the Second International Meeting of High-Ranking Officials Responsible for Security Matters,[3] and, conjointly with the SCO, the Code of Conduct in the Field of Ensuing International Information Security, circulated in 2011 at the 66th Session of the UN General Assembly as an official UN document.[4]

Given the dynamics of negative trends in the digital environment, the imperative now is to put the ongoing general legal discussion in the international community on a practical footing, with an eye to practical results. It is important to do this before a "point of no return" will have been passed on the road to militarization of information space.

NOTES

[1] Earlier in the bienniums 2004-2005, 2009-2010 and 2012-2013.

[2] Statement at the meeting of the First Committee of the UN General Assembly, October 2013.

[3] Convention on International Information Security (Concept) adopted on September 22,

2011: http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/ 542df9e13d28e06ec3257925003542c4!OpenDocument

[4] The Code of Conduct in the Field of Ensuring International Information Security: Letter dated September 12, 2011 from the permanent representatives of Kazakhstan, Kyrgyzstan, China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General. A/66/359 // http://rus.rusemb.org.uk/data/doc/international-coderus.pdf

Key words: international law, international information security (IIS), information and communication technologies (ICT)