MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY
UKRAINIAN FEDERATION OF INFORMATICS

PROCEEDINGS

OF THE V INTERNATIONAL SCIENTIFIC CONFERENCE

ADVANCED INFORMATION SYSTEMS AND TECHNOLOGIES

AIST-2017

(Sumy, May 17–19, 2017)

SUMY
SUMY STATE UNIVERSITY
2017

International Legal Measures Against Information Warfare

Vladyslava Zavhorodnia[1], Maria Kuntsevych[2], Alla Vasylenko[3]
Sumy State University, [1]v.zavhorodnia@uabs.sumdu.edu.ua, [2]m.kuntsevich@uabs.sumdu.edu.ua

***Abstract* – The paper explores possible international legal measures against information warfare and ways of international law application to interstate informational conflicts. The authors attempt to formulate legal definition of informational warfare and identify its essential features. Two types of hostile actions on the criterion of targeting are distinguished as humanitarian and cyber forms of information warfare. The conclusion that the article's authors draw is that the contemporary international law does not establish an appropriate legal regime to information interstate conflicts. A universal international treaty is needed in order to prevent states from information aggression. The concept of its aims and main provision is also suggested.**

***Keywords* – information warfare, information aggression, cyber-attacks, international legal measures against information warfare.**

I. INTRODUCTION

In the XX and at the beginning of the XXI century creation of an alternative world picture and an alternative reality for inhabitants through informational technologies became a common practice for authoritarian and totalitarian states. The majority of those people simply consume proposed information and don't want or for various reasons aren't able to analyze various sources. Democratic states generally don't use such practices, but also makes extensive use of informational resources in political or military purposes. Thus, the use of information technologies had become a real practice of international relations, but wasn't in any way dealt with within the realm of international law.

The informational technologies as well as all achievements in the civilization of mankind could be used both for the common good and for causing harm. A new cyber weapon has appeared, capable of destruction of the whole state's informational structure. Moreover, several states (Estonia, Iran, Germany, USA and others) had already been a subject of cyber-attack. British journal «The Economist» already in the year 2010 defined cyberspace as 'the fifth domain of warfare, after land, sea, air and space'[1].

Hostile propaganda informational psychological influence on society through telecommunication technologies fully experienced by Ukraine is a real threat to sovereignty, independence and territorial integrity of the states. At the same time, legal mechanisms allowing providing legal certainty in such relations between the states, avoiding information wars and enquiring international responsibility, those are not provided by the international law. This article focuses on defining possible international legal measures against information warfare and ways of international law application to relations between states resulting from informational conflicts.

II. THE LEGAL CONCEPT OF INFORMATION WARFARE

The nature and extent of international warfare consequences had profoundly changed after appearance of Internet. Before this event false information emanating from disinformation campaigns as instruments of propaganda has used as a main tool of informational war. Internet appearance led to emergence of the notion of "cyber-attack", targeted both at information itself and a whole information system. New bases for the propaganda had become social networks and Internet media resources. While Internet becomes a space for many social activities cyber-attacks pose a great threat to the national security of each state. Computer viruses can be a tool of attacks on servers of banks, state bodies, and life support system of cities, control systems at nuclear facilities, chemical plant and other potentially dangerous objects. Thus, in modern world the informational technologies could be used as a real weapon in interstate conflicts. The main problem is to enquire international responsibility and to find the persons responsible for the hostile informational actions, because determining the occurrence of an act of the informational aggression is always difficult. Therefore, states always deny their responsibility for such hostile actions, using the advantages of lack of appropriate legal regulations.

Definition of the notion of "informational war" and making necessary international legal norms are a very difficult task, insofar as the attention of scientists recently was mainly paid to the problem of private cyber-attack avoidance [2; 3; 4]. We contain that information warfare is a state of emergency due to actions causes or capable to cause the threat to informational security and targeted both at information itself (its distortion, change or destroying) with the goal of psychological influence on inhabitants and a whole information system and information processing tools of other state in order to disrupt normal operation of informational systems and to lead difficulties in work of authorized users.

There are several essential features of information warfare:

- total impact (effect of information weapons or related technologies mostly isn't individualized; it usually targeted at info systems, thereby causing

harm to the whole country's population);

- there is a significant differences between information warfare and traditional war (enemy doesn't cross the boundary, it is difficult to prove the fact of state sovereignty violation; there is no bloodshed, but the systems operation is blocked and critical information infrastructure is disrupted or destructed);
- methods or means of information warfare are hostile, but not always unlawful (the outbreak of cyber-attack could take place in a great amount of information requests targeted at one informational system);
- tracing the origins of cyber-attacks is very difficult;
- a global character of threat (cyber-attack targeted at one state could become a serious threat to the human community, so far as the network of one state is closely linked to networks of others and its consequences almost always are unpredictable).

The main distinguishing between the information warfare and cyber-attack targeted at private networks is based on criteria of subject of hostile actions. It is possible to assimilate information warfare to a specific type of armed conflict. The role of its parties could be played by states, state-like entities and international organizations. The participants of the information warfare are individuals and could be divided into two groups: those who directly participated in hostilities (combatant) and non-combatants. Cyber-attack could be initiated by subject can not be considered as a part of international warfare. In such case hostile actions should be assimilated to cybercrime and entail criminal responsibility. Information warfare as state of emergency caused by unlawful acts of other state targeted at information security. These hostile actions (form of information warfare) could be divided into two types on the criterion of targeting: ***humanitarian*** and ***cyber***. Humanitarian forms include acts targeted at people minds, modification or distortion of informational world picture, such kind of worldviews transformation which is advantageous for belligerent in the conflict. This form of information warfare can be manifested itself mostly in hostile propaganda in order to influence psychologically on inhabitants of foreign state or to destruct unfavorable or important information. Cyber forms include acts targeted at systems of receiving, processing and distributing information. It should be mentioned that such approach is rather nominal, therefore all-out information war should be waged with coordinated measures of both types.

III. The Legal Provision of International Information Security

Global security issues had been discussed extensively at the international level in the last decade of 20th century. In 1998 the UN General Assembly adopted the UN Resolution A/RES53/70, entitled 'Developments in the field of information and telecommunications in the context of international security'. The revised resolution A/RES/54/49 of the same title was adopted in 1999. It pointed to the danger of informational threats in both civil and military fields. Subsequently, numerous resolutions had been adopted and the General Assembly remains actively seized of this matter.

Internationally legally binding instruments in the field of cybersecurity are elaborated in the framework of the Council of Europe. There are Convention on Cybercrime (2001) and Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003). The Convention on Cybercrime was the first successful attempt to resolve the issues of information security. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. The Treaty seeks to prevent and eliminate the crimes committed via the Internet and other computer networks, but it does not deal with the rules of international warfare.

At the national level the cyberspace policy of United States is of interest. It is based on the vision that the United States reserves the right to use all necessary means against hostile acts, including significant cyber-attacks, directed not only against the US government or military but also the economy. The significant consequences of cyber operations are: loss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States. A retaliatory strike in response to an attack could be launched after Presidential approval [5].

The European Union has also some achievements in cybersecurity regulation. The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016. The Directive provides network and informational strategy. It establishes a duty on Member States to adopt national provision of responding to cyber-attack and exchanging of information.

In 2016 the European Parliament adopted the Resolution on the EU strategic communication to counteract propaganda against it by third parties. The resolution stressed that the EU, Member States and citizens are under growing, systematic pressure to tackle information, disinformation and misinformation campaigns and propaganda from countries and non-state actors, such as transnational terrorist and criminal organisations in its neighbourhood. The Resolution is not a legally binding document, and does not have an enforcement mechanism. It initiates the creation of strategy to counteract anti-EU propaganda and the

adoption of measures to provide a target audience with adequate and interesting information about EU activities.

As evinced by the above overview nowadays States have not agreed on establishment of international mechanisms to counter the threats of information warfare at both universal and regional level. Moreover, there is no common approach on provision information security, restricting hostile propaganda, and prevention cyber-attack related to inter-state relations

In this context the provisions of the Tallinn Manual on the International Law Applicable to Cyber Warfare are of considerable interest. The Manual was developed by NATO's Cooperative Cyber Defense Centre of Excellence and presented in 2013. It is not a regulatory document and does not represent the official policies of NATO. This non-paper is based on existing treaties relating to the law of armed conflict, international law on State responsibility and other provisions of the international law. The Manual is an attempt to develop an international legal mechanism applicable to cyber operations, both conducted by and directed against states. It defines legal concept and types of cyber-attack, establishes criteria for distinguishing between military and nonmilitary targets, regulates the means and methods of cyber warfare. The protections of children, journalists, medical and religious personnel, UN's personnel, natural environment, cultural property, and objects indispensable to survival are also setted.

The second edition of the Tallinn Manual has been drafted in 2017. Tallinn Manual 2.0 adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis, and that fall below the thresholds of the use of force or armed conflict. As such, the 2017 edition covers a full spectrum of international law as applicable to cyber operations, ranging from peacetime legal regimes to the law of armed conflict. The analysis of a wide array of international law principles and regimes that regulate events in cyber space includes principles of general international law, such as the sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialised regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law are examined within the context of cyber operations.

Despite no binding force, Tallinn Manual becomes an influential resource for legal advisers around the world. But it should be noted, that both versions on Tallinn Manual do not cover issues of hostile propaganda in cyberspace.

IV. THE PERSPECTIVES OF INTERNATIONAL LEGAL MECHANISM CREATION

Global information space should be considered as the common heritage of humankind, including the fair and equitable sharing of benefits. Therefore the information warfare should be strictly prohibited by international law. The development of international principles of behavior in cyberspace is very complicated. It should be possible to use an analogy in international law to create appropriate legal measures against information warfare. International law establishes legal regime of international armed conflicts, provides the orderly use of outer space, the high seas and other areas, concerning the national interests of all States. Therefore existing body of principles and legal standards in these fields can be applied to the problems of international information security. It should be possible to identify the definition of information aggression. As stipulated in the Charter and in United Nations resolutions the 'aggression' is use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. The UN's Resolution 'Definition of Aggression' mentions acts, regardless of a declaration of war, qualified as an act of aggression (Article 3). The information aggression might be defined in the similar way. Without claiming to provide a comprehensive analysis of information aggression we will try to indicate its essential features:

- it is an attack by one State against another;
- an aggressor State attacks information and communication technology systems and infrastructure, commits acts characterised as cyber and/or humanitarian type of information war;
- there is an evidence to conclude that perpetrators (hackers, dishonest journalists, bloggers, owners of 'fake' pages in social networks and others) are in any way associated with the state, and government structures are involved in cyber-attack or hostile propaganda;
- the perpetrators within the jurisdiction of State impinge on the sovereignty and information security of another State with impunity, as they have constantly been protected and sheltered from legal accountability by aggressor.

As Shackelford notes, cyber-attacks like nuclear warfare, do not discriminate between combatants and noncombatants, nor do they pass the test of proportionality. If the use of nuclear weapons is subject to the rules of the international law, so too should cyber-attacks. Nuclear weapons are not declared illegal, but methods and means of warfare which would result in unnecessary suffering to combatants, are prohibited. This principle is just as applicable to cyber war as it is to nuclear war [6]. Cyber-attacks like nuclear warfare cause mass destruction. They do not distinct military and civilian targets and can destroy objects indispensable to survival. Complete destruction of nuclear weapons is not required by the Treaty on the Nonproliferation of Nuclear Weapons. But its proliferation is prohibited. A similar approach could also be used to malicious software. It is

not practically possible to prohibit the development of it. However, it could be argued that the prevention of the proliferation of malware is the most effective manner of protecting information security. Legal provisions relating to informational warfare should be aimed at neutralizing the threats of cyber-attack. It should be possible to achieve an interstate agreement on prohibition hostile propaganda, provided that it would be adequately defined. The treaty must contain clearly established criteria and parameters set out in to identify hostile information influence. Four elements are needed in order for the acts to be qualified as hostile propaganda: firstly, systematic character of disseminating false information; secondly, the element of intent; thirdly, the specific purpose; and lastly, the involvement of a State official, at least by support or acquiescence.Although there is some resemblance between the cyberspace and outer space, both of them are incredibly vast areas of the international commons. International law does not permit outer space or cyberspace to be nationalized. Space and telecommunications systems are also intertwined, including in such functions as communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence. 1967 UN Outer Space Treaty analysis allows adapting its provision to the needs of the international legal regulations on information warfare, especially regarding: the prohibition of occupation of outer space (it can be ascertained that obtaining control over information systems of the state by aggressor could be seen as an occupation of information space); freedom of exploration and use of outer space (every individual should be guaranteed the right to Internet access, understood to mean a right of unlimited access to informational resources and their using for his or her own advantage with the exception of violation of human rights or causing harm to a legally protected interests); use of outer space exclusively for peaceful purposes (use of information networks for peaceful purposes, prohibition of information aggression);international liability for damage caused by space objects (analogically state should be responsible for the damage caused by informational objects (computer programs, computer viruses etc.) those had been loaded to the network by it).

CONCLUSIONS

The certain international law provisions could be applied to cyber-attack and hostile propaganda, yet they are unable to ensure comprehensive legal measures against information warfare. The international community's efforts should focus on the conclusion of a universal international treaty and establishing of appropriate legal regime in order to prevent information warfare. The treaty should include 1) legal definitions of information warfare and information aggression; 2) prohibition of intentional hostile propaganda and using of cyber weapons; 3) responsibility of States for information aggressive acts; 4) the allocation of the burden of proof in information warfare matters; 5) the rationale for the use cyber-attack in response. Self-defense attack should be allowed when other means failed; 6) the obligation of the States to penalize intentional and/or recurrent acts of disseminating false information about another State. Otherwise, the State should be held responsible for information aggression.

Special non-governmental nonprofit organization such as The Internet Corporation for Assigned Names and Numbers (ICANN) which is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet, ensuring the network's stable and secure operation, could be established for combating information warfare. This organization should take role on identification of harming activities on the Internet; take out it's an independent evaluation and block if needed. Incidental disputes and conflicts arisen as a result of blocking the activity of some users should be resolved by independent arbitration tribunal, established for such purposes. In the case of absence of reasonable suspicion that the state is involved, a case should be put on trial at the national court.

REFERENCES:

[1] *Cyberwar. The threat from the Internet*, Economist (July 1, 2010), http://www.economist.com/node/16481504?story_id=16481504&source=features_box1.

[2] O. Radutny "Criminal law measures against Internet trolling", *Internet and Law*, vol. 3(15), 2016, pp. 110-114. (in Ukrainian)

[3] O. Shyrokova-Murarash, Yu. Akchurin "Cybercrime and cyberterrorism as a danger to the informational security: international legal aspect", *Internet and Law*, vol. 3(15), 2016, pp. 76-81. (in Ukrainian)

[4] International standards of cybersafety and their appliance in Ukraine, Round Table Papers, Kharkiv: Pravo,, April, 19, 2016, 88 p. (in Ukrainian)

[5] M. Roscini *Cyber Operations as a Use of Force in International Law*, U. of Westminster School of Law Research Paper No. 16-05, 2015, p. 28.

[6] Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 Berkeley J. Int'l Law. 192, 2009.