

## Formation of the International Information Security System and Development

*Aliiev Olim Aybekovich*

Basic doctoral student of Andijan State University

-----\*\*\*-----

**Abstract:** The article deals with the types of cybercrime and effective methods of its elimination, the formation, development of the international information security system.

**Keywords:** Geneva Convention, information threats, artificial intelligence, cybercrime.

### Introduction

As a result of the globalization of information exchange in the international arena, there is a need to find international mechanisms to reduce the dangerous effects of information flows in the international community. Therefore, the development of the international legal framework of information security has become one of the most pressing issues. The following legislative acts have been adopted within the framework of the global information space:

- Rules of armed conflict established by the Geneva Conventions<sup>1</sup> of 12 August 1949 and The Hague<sup>2</sup>;
- 1973 International Telecommunication Convention;

This convention was adopted in connection with the consequences of the use of information tools and the formation of information fields with specific features of this process.

<sup>1</sup> Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны // [https://www.un.org/ru/documents/decl\\_conv/conventions/geneva\\_civilian\\_1.shtml](https://www.un.org/ru/documents/decl_conv/conventions/geneva_civilian_1.shtml).

<sup>2</sup> Саямов Юрий Николаевич. О Гаагских конференциях 1899 и 1907 гг // Россия и современный мир.- Москва, 2017.-Вып.3

The subject of the UN document "Achievements in the field of information and telecommunications in international security", adopted by the UN on December 4, 1998, was the official beginning of a completely new international legal regime with information, information technology and methods of their use<sup>3</sup>. The UN General Assembly discussed the document in 2000, which recommended the definition and formation of basic concepts such as "information weapons", "information warfare" and "information security".

### Main part

The Okinawa Charter of the Global Information Society, adopted in July 2000 at the G8 Summit in Okinawa, has played an important role in establishing an international legal regime for international information security. This Charter recognized the revolutionary impact of ICT on all spheres of public life.

In 2001, on the recommendation of the UN Economic and Social Council, the UN Secretary-General established the United Nations Information and Communication Technologies Task Force (UNICTTF). The initiative is set to carry out tasks such as "eliminating the global digital divide, bringing the set of actions to a new global level, while ensuring that ICT serves the development of all."

On April 29, 2002, a meeting of working groups was organized in Geneva, at which regional Target Groups for Europe and Central Asia were established. By the end of May 2002, six more such

<sup>3</sup> Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь.- 1999, №2.-С.48.

groups had been established, and the Regional Networks Bureau, with the participation of leading experts, had been set up to formulate a coherent policy for the development of the information society<sup>4</sup>.

On September 22, 2011, the UN General Assembly adopted the Convention on International Information Security. Its main goal is to "take measures to combat ICT, which is used to disrupt international peace and stability, as well as to promote the activities of states in the field of information."<sup>5</sup>

On December 2, 2014, the UN General Assembly adopted a resolution entitled "Achievements in the Field of Information and Telecommunications in the Context of International Security"<sup>6</sup> (A / RES / 69/28). It retains the provisions of the resolution of the same name adopted on December 3, 2012 (A / RES / 67/27)<sup>7</sup> on respect for human rights and fundamental freedoms in the field of ICT.....

In this regard, the number of co-authors of this document has grown from year to year. The number of such states increased to 50 in 2014. The document is of global importance, and its geography covers almost all regions of the globe. This year, the Government Experts Group held its fourth meeting, which was attended by more than 50 countries. The priority of the group's research was to identify threats in the field of ICT, and to formulate ways and means to combat them jointly and collaboratively.....

As a result of these efforts, general agreements have been reached on a number of issues. In particular, the issue of combating current threats to international information security was given priority. He was given many more tasks, such as increasing the capacity of ICT for military purposes, increasing its influence in conflicts, the destruction of important strategic objects that are a source of threats with the help of ICT.

In 2016, at the suggestion of the Russian Federation, a new draft resolution "Achievements in the field of information and telecommunications in the context of international security", co-authored by 84 countries, was adopted. The BRICS, SCO, CIS, Latin America and Asia participated in its development. For the first time, the United States, Japan, EU members - the United Kingdom, Germany, Spain, the Netherlands and France - co-authored the document.

On October 22, 2018, at the 73rd session of the UN General Assembly, the next UN resolution "Achievements in the field of information and telecommunications in the context of international security" was adopted. "While states have a primary responsibility for a peaceful information and communication environment and security, identifying mechanisms to engage civil society, the private sector and academia when necessary, and adopting a draft international code of ethics for international information security can help increase international cooperation," he said." was noted.

The resolution stressed for the first time that international institutions should be the mainstay of global information security, as well as a mechanism to prevent information wars. With the help of international institutions, there is an opportunity to influence the subjects of international law related to international information security<sup>8</sup>.

<sup>4</sup> Convention on Cybercrime (Будапешт, 23 ноября 2001 г.)  
<http://conventions.coe.int>.

<sup>5</sup> Конвенция об обеспечении международной информационной безопасности// [https://www.mid.ru/foreign\\_policy/official\\_documents/-/asset\\_publisher/CptICk6BZ29/content/id/191666](https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICk6BZ29/content/id/191666).

<sup>6</sup> См.:Резолюция от 2 декабря 2014 г. A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: <https://documentsdds-ny.un.org/doc/UNDOC/GEN/N14/662/43/PDF/N1466243.pdf> (дата обращения: 16.11.2019).

<sup>7</sup> См.:Резолюция от 3 декабря 2012 г. A/RES/67/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: <https://documentsdds-ny.un.org/doc/UNDOC/GEN/N12/480/24/PDF/N1248024.pdf> (дата обращения: 16.11.2019).

<sup>8</sup> См.:Резолюция ООН от 5 декабря 2018 г. A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/RES/73/27](https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/73/27) (дата обращения: 16.11.2019).

On March 12, 2021, the UN Open Working Group adopted a report entitled “Achievements in the Field of Information and Telecommunications in the Context of International Security”. The report was adopted by mutual agreement of all participating states. In addition to being an analytical document on the results of the past two years from 2018, the report also reflected the assessments of the international community on the situation in the cyber space in a mutually agreed manner.

Under the mandate of the Open Content Working Group (OCWG), the report covered the following topics: -existing and potential threats; - norms, rules and principles of responsible behavior of states;

- issues of application of international law;
- confidence-building measures; - Measures to increase the capacity in the field of ICT;
- Issues of organizing regular institutional dialogues on information security.

OCWG participants noted the inevitability of the use of ICT in conflicts between states, and the growing concern about the use of such opportunities by states, as well as non-governmental entities. The report also published an analysis of the consequences of devastating attacks on serious information structures. In particular, the importance of protecting healthcare infrastructure during the COVID-19 pandemic was noted. Protecting this sector is important for both the international, interstate and private sectors.

In the last five years, new and improved forms of cybercrime have begun to appear in the international information space. This, of course, started to cause a lot of problems. Artificial intelligence has also begun to be used to increase the effectiveness of malicious software. In these processes, the SI-algorithm is used to bypass the protection system, to increase the capacity of the existing malicious system, to replenish it.....

SI-algorithms are emerging with the ability to analyze large amounts of data to find and identify phone numbers and credit card numbers. Such systems can analyze images and videos in texts other

than text. According to experts, SI may be used in the future in connection with social engineering, as well as in extortion through automated calls. SI systems can create any person's voice when making voice messages, thereby causing great harm to their victims.<sup>9</sup>

Global cybercrime losses and spending in this area will increase by 50 percent over the next two years to \$ 1.1 trillion by 2020. dollars (in 2018, the damage caused by cybercriminals was \$ 600 billion) or more than 1 percent of world GDP. As the world goes digital, cyber attacks are on the rise. They are the new digital world and 4.0. poses a direct threat to industrialization. Currently, cyber attacks are among the five global threats - climate change, epidemics and natural disasters.

The World Economic Forum estimates that the economic damage from cyber attacks will reach \$ 2.5 trillion by 2020. dollars. According to forecasts, this figure will reach 8 trillion in 2022. dollars. Pest viruses such as NotPetya and WannaCry have estimated the damage from cyber attacks at \$ 10 billion. dollars.

Of course, the increase and escalation of cybercrime and cyber-attacks in the international arena, the improvement of information wars, their spread to the regions have led the UN and other international organizations to make major changes in the field of information security. That is why for almost a quarter of a century, international information security has developed as a concept, practice and protection factor.

### Conclusion

In short, the rise of cybercrime has prompted nation-states to work together to improve and enhance international information security around the UN. Of course, the developed countries took an active part in these difficult and arduous processes, spared no effort and resources in this area. Over the past period, an international security system has been

<sup>9</sup> Фетисов В. Европол и Trend Micro рассказали, как хакеры используют ИИ в своих интересах. 26.11.2020 г. // <https://3dnews.ru/1026363/evropol-i-trend-micro-rasskazali-kak-hakeri-ispolzuyut-ii-v-svoih-interesah>.

formed, which has covered most countries in the world.

#### REFERENCES:

1. Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны // [https://www.un.org/ru/documents/decl\\_conv/conventions/geneva\\_civilian\\_1.shtml](https://www.un.org/ru/documents/decl_conv/conventions/geneva_civilian_1.shtml).
2. Конвенция об обеспечении международной информационной безопасности // [https://www.mid.ru/foreign\\_policy/official\\_documents/-/asset\\_publisher/ptICkV6BZ29/content/id/191666](https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/ptICkV6BZ29/content/id/191666)
3. Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь.- 1999.
4. Резолюция от 2 декабря 2014 г. A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: <https://documentsddsny.un.org/doc/UNDOC/GEN/N14/662/43/PDF/1466243.pdf> (дата обращения: 16.11.2019).
5. Резолюция от 3 декабря 2012 г. A/RES/67/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: <https://documentsddsny.un.org/doc/UNDOC/GEN/N12/0/24/PDF/N1248024.pdf> (дата обращения: 16.11.2019).
6. Резолюция ООН от 5 декабря 2018 г. A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/RES/73/27](https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/73/27) (дата обращения: 16.11.2019).
7. Саямов Юрий Николаевич. О Гаагских конференциях 1899 и 1907 гг // Россия и современный мир.- Москва, 2017.- Вып.3(96).
8. Фетисов В. Европол и Trend Micro рассказали, как хакеры используют ИИ в своих интересах. 26.11.2020 г. // <https://3dnews.ru/1026363/evropo-l-i-trend-micro-rasskazali-kak-hakeri-ispolzuyut-ii-v-svoih-interesah>.
9. Convention on Cybercrime (Будапешт, 23 ноября 2001 г.) // <http://conventions.coe.int>.