INTERNATIONAL COOPERATION IN THE CYBER SECURITY FIELD IN UKRAINE

Nazarenko D.I.,[1] Vynohradov D.O.[1]
[1]National Aviation University, Kyiv
Supervisor - Martyniuk H.V., PhD, Associate Professor

Cybersecurity is a priority topic for all states and Ukraine is no exception. With the development of technology, the number of cybercrimes has increased, according to experts, over the past few years, the total losses from cyberattacks were $ 4 trillion. [2]

The priority issue is the creation of a solid security system for the transfer, processing and storage of data between countries of the world. Ukraine's experience shows that countering serious and persistent cyber threats and attacks requires enhanced cooperation at several levels [1] - between national authorities, the private sector and international partners, to build the necessary capacity and effectively respond to such threats.

The development of new technologies in the country depends on the comfort of legislation in this area. Here the legislation, on the author opinion, should be such that creates favorable conditions for development. The legislation of Ukraine contains a law "On the basic principles of ensuring the cybersecurity of Ukraine". Chapter 14 of this law deals with international cooperation in the field of cybersecurity.

There are 4 steps to achieve international cooperation[2] :

1.Convention on Cybercrime:

The Convention aims principally at:

- Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form;
- Setting up a fast and effective regime of international cooperation.

Ukraine has ratified the Convention on Cybercrime.

2. Representation in international cooperation formats:

Requirement: the government is regularly represented in a cooperation format that is dedicated to international cyber security (for example First and Impact Alliance). Our country has fulfilled this requirement

3. International cyber security organization hosted by the country:

Requirement: a regional or international cyber security organization is hosted by the country. Our country has not met the requirement to fulfill there must be three. To fulfill this requirement, the government needs to have a Cybersecurity Strategy of Ukraine. This will enable the country to host a regional or international cybersecurity organization. This will help a lot because the losses in the world from cyber threats are reaching astronomical values.

4. Cyber security capacity building for other countries

Requirement: The country has (co-)financed or (co-)organized at least one capacity building project for another country in the last 3 years. Our country has not (co) financed or (co) organized any capacity building projects for another country. Building capacity for another country will affect the development of the cybersecurity industry as a whole. This will attract large investments from different countries for global projects.

Although international cooperation will cause positive progress, there are also disadvantages. The launch of joint projects will give a powerful impetus to the entire industry. Companies and developers will receive additional resources, government orders. In the coming decades, the world will become completely digital.

Increased digitalization of services and reliance to the internet have brought about the evolution of cyberspace, raising also significant security challenges to governments across the globe vis-a-vis offences against and by means of computer systems. In Ukraine this has been demonstrated most significantly with the large-scale cyberattacks to Ukrainian power companies in December 2015 following attacks to major Ukrainian TV channels two months earlier on the day of local elections.

These incidents fit within the overall trend that Ukraine is witnessing the past years with an increased use of Distributed Denial of Service attacks as well as zero-day vulnerabilities exploited to penetrate and compromise critical infrastructures. The threat landscape analysis also points to targeted attacks on diplomats, law enforcement agencies, defense actors, state enterprises, mass media, as well as politicians and public figures, as well as misinformation campaigns over the Internet to influence the 'physical' world. The impact of these attacks can be significant as they can damage critical infrastructures and hinder the effective functioning of the national authorities. Information and psychological warfare aims at discrediting state power and fosters the conditions for the destabilization of the social and political situation.

Cooperation in the field of cybersecurity involves the creation of a digital alliance by countries. This can lead to the division of the whole world into such alliances and cause new conflicts.

Therefore, the conclusion means that international cooperation in the cyber security in Ukraine has great potential for development and cooperation with other countries of the world.

References:

1. Convention on Cybercrime [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Convention_on_Cybercrime

2. Cybersecurity indicators [Electronic resource]. – Access mode: https://ncsi.ega.ee/country/ua/495/#details