надання статусу біженця та певні недоліки в законодавстві, які ставлять під питання правовий статус біженців.

Список використаних джерел:

1. Волкова С. Г. Правове регулювання статусу біженців в Україні [Електронний ресурс] – Режим доступу до ресурсу: http://radnuk.info/statti/226-admin-pravo/14515-2011-01-18-03-24-45.html

2. Джумаєва К.Б. Проблемні питання визначення поняття «біженець» в Україні [Електронний ресурс] – Режим доступу до ресурсу: http://dspace.univer.kharkov.ua/bitstream/123456789/8419/2/Dgumaeva.pdf

3. Для осіб, що звертаються за захистом в Україні [Електронний ресурс] – Режим доступу до ресурсу: http://dmsu.gov.ua/posluhy/nabuttya-statusu-bizhentsya-abo-dodatkovogo-zakhistu

Repytskyi T.V.
Student,
Matej Bel University (Slovakia)

CYBER WARFARE AND INTERNTATIONAL HUMANITARIAN LAW

Cyber attacks are not what makes the cool war 'cool.' As a strategic matter, they do not differ fundamentally from older tools of espionage and sabotage Noah Feldman, Harward Law School

The development of modern technologies is not only influencing our modern life, usually it is two steps ahead of us and the laws we are used to follow. Since the establishment of Internet, and its broader usage, not also a variety of opportunities became available, but also the crime sphere is profiting. It was just a matter of time to see when Internet and electronic system would become another and dangerous kind of warfare. Storage of sensitive information on networks has given birth to cyber espionage against governments and cyber economic warfare against businesses [1, p. 8].

It is already tricky from the very beginning, as officially there is no definition of what is understood under the term «cyber warfare». One of the U.S. officials describes «cyber warfare» as «actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption» [2]. That is probably the most short, but also precise definition. Cambridge dictionary, defines

«cyber warfare», as «the activity of using the internet to attack a country's computers in order to damage things such as communication and transport systems or water and electricity supplies» [3]. It basically means that it is an attack which starts in electronic systems, but can cause real-world harm. That is quite an important element of defining, meaning that a simple attack on some governmental web-page would not be considered as means of cyber warfare, but rather a «cyber attack». Some wars were won without causing real-harm and sufficient destructions, as well sabotage of some state-important buildings or infrastructure can cause more real harm than war.

There are different techniques of cyber warfare, but we can outline the most significant ones:

- Espionage and national security breaches.
- Sabotage.
- Electrical power grid.
- Attacking critical infrastructure.
- Equipment disruption.
- Distributed Denial-of-Service Attacks.

In recent years, world has faced «good» examples of how cyber warfare can be used, as well an opportunity to determine what capability it has. The most prominent cyber warfare usage includes:

- 2014 attack on Ukraine.
- 2011 attack on South Korea.
- 2010 attack on Iran.
- 2008 attacks during South Ossetia.
- 2007 attack on Estonia.

Even though these attacks were mainly connected with espionage and sabotage of work of some state authorities it is clear, that a potential of cyber warfare is much higher.

Why do countries will make efforts to use cyber warfare more intensively in the future? We must say that the main reasons for that would be:

- Sudden effect of the attack.
- Wars can be won on distance.
- It's much cheaper than ordinary methods.
- Quantity of one specialist in IT and his work can overcome power used by thousands of ordinary soldiers.
- Reduced the factor of loss of specialists.

- State may start the war, using cyber dimension, remaining in secret for some time.

To conclude the above said, not only scholars, but governments have to pay more attention to the arising issue of cyber warfare. Millions of dollars are spent nowadays not only on development of methods to attack, but also to defense of possible attacks. It appears that cyber warfare is just a ticking bomb, where no one knows when it will explode.

At the present time, there is no legal document, which would deal with the «cyber warfare». The most comprehensive research, on our opinion, on this issue is called Tallinn Manual, which is an academic, non-binding study on how international humanitarian law applies to cyber warfare. By cyber warfare, we're talking here solely about means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of international humanitarian law (IHL). It does not apply to every kind of activity called «cyber attacks» in common parlance [4].

The Council of Europe has taken the most direct approach to regulating a subset of the cyber security problem–in particular, cyber crime – of any international organization to date. As the first international treaty on crimes committed using the Internet and other computer networks, the 2001 Council of Europe Convention on Cybercrime («Cybercrime Convention») promulgated «a common criminal policy aimed at the protection of society against cybercrime,» primarily through legislation and international cooperation [5].

It is important to mention, that means and methods of war have evolved since the Geneva Conventions were drafted in 1949, but IHL continues to apply to all activities conducted by parties in the course of armed conflict, and must be respected. It cannot be ruled out, however, that there might be a need to develop the law further to ensure it provides sufficient protection to the civilian population, as cyber technologies evolve or their humanitarian impact is better understood [4].

The question would be, how effective would such legal document (in a form of convention, regulation or treaty) be. As mentioned above, the technologies are usually ahead of developments in legal terms, and the international discussion is way too slow and unwilling to make a common decision, as well as it is simply beyond the different interests. Unfortunately, the political factor is playing a key role in legal determination of such prominent case of present and future importance.

According to the article 36 of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims

of International Armed Conflicts (Protocol I), 8 June 1977, «in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party» [6]. This basically means that the law of armed conflict applies to cyber warfare.

By adopting a regulatory document on the issue, more questions will be also put on the table for discussion. For example, in what cases attacked state has the right on its part to use violence in response to a digital attack? And whether it can be done in the form of air strikes? The main question though, is whether states are interested in playing the cyber war game fair?

References:

1. Andrew F. Krepinevich, Cyber Warfare: A «Nuclear Option?», Washington, DC: Center for Strategic and Budgetary Assessments, 2012.

2. Richard A. Clarke, Cyber War: The Next Threat to National Security and What to Do About It, Ecco, 2012.

3. Cambridge online dictionary. [Електронний ресурс]. Режим доступу: http://dictionary.cambridge.org/dictionary/business-english/cyber-warfare

4. Interview. «The law of war imposes limits on cyber attacks too». [Електронний ресурс]. Режим доступу: https://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm

5. Council of Europe, ETS № 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23, 2001), entered into force July 1, 2004, [Електронний ресурс]. Режим доступу: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

6. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. [Електронний ресурс]. Режим доступу: https://www.icrc.org/ihl/WebART/470-750045?OpenDocument