TECHNOLOGICAL DEVELOPMENTS IN CYBERSPACE AND COMMISSION OF THE CRIMES IN INTERNATIONAL LAW AND IRAN

Aramesh Shahbazi, Allameh Tabataba'i University

ABSTRACT

Technology has always been a problem for legal systems. Indeed, while law and technology are two distinct areas for discussion, both are interwoven and no discussion is complete without recognizing the other. In the context of legal profession though new technology presents exciting opportunities for legal advancements, it also presents a lot of uncertainty and vagueness in authorized acts and omissions especially in the field of criminology. In this case, the cyber space could be considered as a safe environment for criminals to commit criminal acts by utilizing the network security gaps and abusing available ambiguities due to the lack of enforceable forces and some inefficient binding force. Nowadays, the significant growth of cyber criminals through hacking the data, influencing the computer networks, espying the cyber space and even terrorist acts are considered as a serious threat for to the states in their national and international affairs. However, given the serious differences between the two legal systems of national law and international law in terms of structure, subjects and the objects, and also in conclusion of the systematic development of national law to international law, one can believe in dichotomy of these two legal systems in criminalization and combating the crimes at national and international levels.

The most important question of this article is that what is the impact of the technological developments on commission of the crimes in cyberspace in national law and at international level? To provide a concrete answer, I will just focus on Iran's legal system and compare the international legal system with Iran's legal system in criminalization, responding and applying the punishments for the cybercrimes. The hypothesis to answer the main question of this article is that due to many differences between Iran's legal system and international law, and while technological developments could facilitate committing the crimes in cyberspace, proper policy-making and appropriate co-operation among states in international law and appropriate law-making in Iran could overcome the threats of cyber crimes.

Therefore, in this article, by a comparative method, I will examine two different legal systems in criminalization and applying criminal responsibility to criminals and then I reach the conclusion that a long way to an idealistic confrontation of cybercrimes has remained.

Keywords: Technological Development, Cybercrimes, International Law, Iran's Legal System, Criminal Responsibility.

INTRODUCTION

Since the end of the second half of the twentieth century, which access to Internet and cyberspace has been increased, and since the use of information technology has been improved,

using technology in daily life has become popular among individuals and it was expected that everyday life and activities could be hardly possible by lacking of technology.

In fact, it can be argued that in this society, the growth of the use of information networks is not confined to the uses of everyday life; and furthermore, many of scientific activities, discoveries and inventions by politicians, lawyers, and physicians, relies on using information data and by assistance of technological software and computer applications.

However, at the same time that these developments have opened new horizons in today's human life, they have also brought serious challenges in some areas of international law. Therefore, while for example in traditional international law the invasion of the territorial integrity of a state was possible only through armistice weapons, today is it simply possible by using security radars or through advanced cyber espionage operations. On the hand, if the crimes have previously carried out through the organized trans-boundary criminals such as the Mafia bands, terrorist groups and by weapons of mass destructions, today it is possible easily by robbery of the secret user information, access to confidential information through the use of advanced computer technology or manipulation of the individual's private data without any need for physical presence in the crime location.

Therefore, it could be argued that:

> *"The Cyber-crime is the achievement of recent technological evolutions."*

In this situation, while criminals have been quick to adopt new technologies, law enforcement has moved relatively slowly. Moreover, cyber criminals customarily operate beyond the legal jurisdiction of the state; therefore it is hardly possible for the victims or even international community of states as a whole to recognize the offenders. This difficulty is an important factor in commission of the crimes in cyberspace. In this regard, it can be argued that

> *"The evolution of some of the concepts of the traditional international law, which is due to advances in technology and in cyberspace, has brought many challenging questions ahead of states and international lawyers."*

Some of the most serious questions are focused on crimes, such as crimes that are not committed by states but by individuals that are out of the territory of states or by criminals beyond the jurisdiction of the victim state even through the physical or mental assistant of any foreign state. In this paper, I will discuss the necessity for international co-operation and its legal requirements in dealing with cyber-crime, and examine the concept and scope of cybercrime, and then I will explore the realization of cybercrime and examine the capabilities and necessities of contemporary international law and the law of Iran in the field of cybercrimes. Finally, I will evaluate the international cooperation in this regard, as well as reaching the conclusion that Collaboration between States, intelligence agencies and law enforcement officers is so critical to prosecuting cybercrime, therefore the new international organizations in the context of international law and new institutions in Iran's legal system can pave the road for a better confronting with cyber-crimes.

CONCEPTUAL FRAMEWORK

In this paper, I try to provide the appropriate context for the analysis of the cybercrimes in Iran's legal system, and then by a comparative view, I will compare this legal system with international legal system. In this regard; it is first necessary to examine the concept and the scope of cyber activities, cyber operations, cyber warfare and the cybercrimes. Then I will scrutinise the framework and the status of the responsibility regime in each different system.

Obviously, given the serious difference between the two legal systems of Iran and international law in terms of structure, subjects and the objects, on the one hand, and on the other hand, with regard to the systematic development of national law rather than international law, one can believe in dichotomy of these two legal systems. Thus, on one hand, development of the national legal system, and its integrity, and on the other hand, underdevelopment of the concepts in international law and also its diversity in rules and institutions has been caused to two different legal systems in combating the cyber-crimes.

Cyber-Space Activities

The cyber space is considered to be the environment in which computer communication takes place in the context of digital communication between different users (Valeriano & Ryan, 2015). In this way, it can be claimed that:

> *"Cyberspace could be considered as a common place to all computer networks around the world."*

Therefore, nonetheless the Cyberspace is an area beyond the boundaries of national governments, the challenges and disputes of the international community in exploiting and recognition of the its legal system and its implications are in any case within the boundaries of national states (Brenner, 2013).

After the 4th technological revolution, the States believe that traditional wars have been replaced by cybercrime attacks, which, in addition to less costs and undesirable consequences than conventional wars, are easier to indirectly achieve to their intended ends (Kesan & Carol, 2012). Therefore, while the cost of starting a cyber-war usually involves the cost of training and using cyber soldiers and the purchase of the software and hardware, the traditional wars are more expensive.

However, it is worth mentioning that a successful cyber-attack, as a traditional war, could target critical and serious systems, including hospitals, government defences, financial systems, transportation, and fundamentals of a State. A successful cyber-attack in these circumstances could have very damaging and catastrophic impacts. For example, cybercrime attacks on networks and shipping systems could cause air strikes or collisions between trains, or in the case of a cyber-attack on water services, they may also lead to flooding and huge damages.

Therefore, with the advent of low cost computing devices, cyber attackers can exert an adverse impact disproportionate to their size. They do not require sophisticated weaponry, and neither do they have to build expensive platforms such as stealth fighters or aircraft carriers, in order to compromise the network of interest and pose a significant threat (Lynn & William, 2010).

In three next subsections, I will briefly examine the differences between different concepts of cyber activities. The first is cyber operation, which is more widespread while its threshold is less than waging war; the second is cyber-attack which normally leads to a cyber-warfare and the last is the cyber-crimes. In this article I will confined the scope of the debate to cybercrimes and its subsequence in domestic law of Iran and international law.

Cyberspace Operations

However, as a rule, the tensions between governments in cyberspace are typically recognized in a general context of the *"cyber operations".* This generic term, which is very similar to cyber operation, is so flexible that it may cover a variety of actions, without any necessarily intention to waging the war. It seems this is the most challenging achievement of the technological developments for international law which brings many unanswered and complicated issues in front of us.

As it is clear, cyber activities in the form of cyber-attacks and cyber warfare could be considered as the wrongful acts, by breach of the principle of non-intervention in domestic affairs of the other states or the infringement of the principle of non-use of force. However, a crucial unresolved issue with respect to sovereign rights of states is whether cyber operations that neither cause physical damage nor amount to an intervention nevertheless violate the targeted state's sovereignty (Michael, 2014). There has not yet been responded in international law, however in the context of the cyber-crimes, it could be argued that because of the victims of the crimes, which are individuals in the first place, the crime has been occurred.

Cyber Attacks

Cyber-attacks are understood as:

> *"Operations to disrupt, deny, degrade, or destroy information resident in computers, computer networks, or the computers and networks themselves".*

This definition is based on the US military doctrine, Matthew C. Waxmans definition and the definition made by Yoram Dinstein (Sophie, 2014). Therefore the Cyber-attacks, which also known as those intentionally computer network attacks, could destroy information and computer networks seriously.

The seriousness of cyber-attacks and the vulnerability of states risking being a victim of cyber-attacks have also been recognized by the international community[1]. The UN panel of governmental experts acknowledges that:

> *"Cyber-attacks pose an enormous threat against "public safety, the security of nations and the stability of the globally linked international community as a whole" (Sophie, 2014).*

Cyber Crimes

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world.

> *"Cyber-crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime" (Kamini, 2011).*

Computer crimes include unauthorized violations of the network and theft of intellectual property and other related information.

A generalized definition of cyber-crime may be:

> ***"****Unlawful acts wherein the computer is either a tool or target or both"*

The computer may be used as a tool in the following kinds of activity-financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases-unauthorized access to computer/computer system/computer networks, theft of information contained in the electronic form, e-mail bombing[2], data didling[3], salami attacks[4], logic bombs[5], Trojan attacks[6], internet time thefts[7], web jacking[8], theft of computer system, physically damaging the computer system (Kamini, 2011).

Cybercrime often has an international dimension. E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient, or illegal content is stored outside the country. Within cybercrime investigations, close cooperation between the countries involved is very important. The existing mutual legal assistance agreements are based on formal, complex and often time-consuming procedures, and in addition often do not cover computer-specific investigations. Setting up procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital (Cybercrime Legislation, 2012).

A number of countries base their mutual legal assistance regime on the principle of "*dual criminality*". Investigations on a global scope are generally limited to those crimes that are criminalized in all participating countries. Although there are a number of offences-such as the distribution of child pornography-that can be prosecuted in most jurisdictions, regional differences play an important role. One example is other types of illegal content, such as hate speech. The criminalization of illegal content differs in various countries. Material that can lawfully be distributed in one country can easily be illegal in another country. The computer technology currently in use is basically the same around the world. Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardization, the network protocols used in countries on the African continent are the same as those used in the United States. Standardization enables users around the world to access the same services over the Internet.[9]

The Technological Developments and Commission of the Crimes in Cyberspace

Some believe that the term industrial revolution is initially defined as:

> *"[…] the period of time during which work began to be done more by machines in factories than by hand at home".*

The advances in science and technology have continuously supported the development of industrialization all around the world, and have helped to bring more specific and explicit meanings to this term over the years (Yongxin et al., 2018).

At the present time, no universal agreement has been recognized on the restrict definition of the industrial revolution (Maynard, 2015), nonetheless, from the perspective of the technological evolution according to the National Academy of Science and Engineering report four general phases have been identified (National Academy of Science and Engineering, 2013). The first industrial revolution is considered as one of the important advancements in humanity, which started by using water and steam-powered mechanical manufacturing facilities since the end of 18th century. Later, at the start of 20th century, the application of electrically-powered mass production technologies, through the division of labour, was marked as the second industrial revolution. After that, to support further automation of manufacturing, the third industrial revolution began, around mid-1970s, by popularizing electronics and information technology (IT) in factories. In total, these three industrial revolutions took roughly two centuries to develop. In the past few years, along with the increased research attention on the Internet of Things (IoT) and Cyber-Physical Systems (CPS), industry, governments and society in general have noticed the trend towards the "*Fourth Industrial Revolution*" and acted to benefit from what it could provide(Yongxin et al., 2018).

In general, it can be claimed that:

> *"The life of cybercrimes is the same as the life of the computer inventions, since from the very beginning of the invention of the computers; man has been easily able to carry out the crimes in cyberspace.*"

However Contrary to the traditional methods of committing crimes, with the development of technology, crimes are committed in a different way. In this way, normally the offender uses a computer or any other means to disrupt the network, abduction or tampering with the information and, in the case of intentional intent to deliberately commit and not enforce, a cyber-crime is committed.

Below, we have distinguish committing the cybercrimes in two sections of national and international law domain by focusing on Iranian legal system to examine the role of technology in committing the cybercrimes at the both levels.

International Law

In *international* law, the signing of the European Convention on Cybercrime has paved the way for the Council of Europe to take the first step in the international legal struggle against computer crime (Atul, 2005). The Budapest Convention[10] is a criminal justice treaty that generally provides States with:

1. The criminalisation of a list of attacks against and by means of computers;
2. Procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards;
3. International police and judicial cooperation on cybercrime and e-evidence.[11]

From the substantial perspective, the Convention provides for four broad categories of *substantive* offence:

1. Offences against the confidentiality, integrity and availability of computer data and systems;
2. Computer-related offences (computer-related fraud and forgery);
3. Content-related offences (child pornography);
4. Criminal copyright infringement.

While in some respects the Convention has proved to be remarkably resilient-capable of adapting to new forms of technology such as botnets-clearly these offences do not encompass the full spectrum of cybercrimes. Notable omissions include identity theft, sexual grooming of children, unsolicited emails or spam and so-called "*cyber terrorism"* (Jonathan, 2014).[12]

Iran's Legal System

Legislation in Iran on cybercrime is dated back to 2009. The cyber-Crime Law was adopted in 2008 and was finally implemented after the Guardian Council approval in 2009 (Behzad & Seyeed, 2014). Of course, it should be noted that cyberspace in Iranian legal system sometimes refers to the context in which various types of crimes are committed, and therefore the title is not a specific crime. Article 1 of the Iranian Cybercrime Act states that:

> "*Anyone who illegally access to data or computer systems or communications associated with protected security measures shall be imprisoned from ninety one days to one year, or 20 to 100 million Rials as cash penalty".*

The same is about forgery. As stated in Article 6 of the same law:

> *"Anyone unlawfully committing the following acts shall be considered as forger and shall be sentenced to imprisonment from 1 to 5 years or penalty of 100 million Rials cash or both."*

1. Changing data citation or creating or entering data fraudulently
2. Changing the data or symptoms in memory cards or in systems and unauthorized modification of the data.

It may be even recognized as a crime contrary to public order, as stated in Article 14 of the Computer Crime Act:

> *"Anyone who produces sends or publishes pornographic content by computer or telecommunication systems or data carriers, imprisoned from ninety one days to two years, or punished for cash payment from 5 million to 40 million Rials, or both."*

Therefore, most of the ordinary crimes can occur in cyberspace, and the type of crime does not affect the definition of cybercriminals or cybercrime.

Response to Cybercrimes, Challenges and Achievements

In fact, in the case of cyber-operations, it will be difficult to recognize the crimes, because it will be challenging to identify the ownership of an attack accurately (Adam, 2013). Moreover, the preparations for cyber-operations are far less visible than that for conventional crimes. For the latter, preparations are usually evident through a military action, hijacking, robbery and etc. but there are no visible signs of preparations when it comes to cyber-operations

(Dieterle, 2013). Therefore the case for cyber criminals seems more difficult to be recognized because of two important factors of the crimes rather to other wrongful acts in cyberspace: first: the ambiguity in criminal intention of the criminals (mens rea), and second the possibility of attribution of the crimes to criminals (actus reus) (Darid et al., 2014).

Moreover, it seems that the complexities and ambiguities in cybercrimes, and the lack of any harmonization in national laws of the states, prevent the necessary and suitable responses against cybercrimes. Some of the most serious obstacles are as below:

1. The lack of any global consensus on the factors and activities that constitute the cybercrime
2. Lack of universal consensus on the legal definition of this cybercrime,
3. Lack of any expertise in the police, prosecuting authorities and domestic or international courts on crimes in cyberspace,
4. Inadequacy of the legal authorities for research and access to computer systems, including the ability to seize and investigate the computer data,
5. The different and various types of cybercrimes in different states,
6. Lack of bilateral assistance and extradition treaties and concrete coordinated mechanisms among states in this regard (Miriam, 2014).

It should be mentions that according to Budapest convention on cybercrime (2001) at the domestic level, both substantive offences and investigative powers may be enacted without recourse to any international agreement. It is when those offences and procedures are to be applied outside of the jurisdiction that international agreement becomes of crucial significance. The ability to carry out investigations affecting the territory of other states, so-called investigative jurisdiction, is addressed in the third chapter of the Convention (Miriam, 2014), and based on the mutual assistance of the states. Some believe that this general principle of cooperation is to be carried out through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws. This reinforces the general principle that cooperation under chapter III does not supersede these other instruments and arrangements. Moreover, it could strengthen the universal recognition of the cybercrimes and lead to better interpretation and implementation of the goals of the documents in domestic affairs of the states.

Therefore, though the international community in two recent decades has witnessed a number of initiatives by international bodies such as the Organization for Economic Cooperation and Development (OECD), Council of Europe (COE), G-8, European Union, United Nations, and the Interpol, in order to harmonize the efforts in combating the cyber-crimes, In the absence of any comprehensive international agreement, the Budapest Convention has been still remained as the most complete international standard against cybercrimes.

Crimes and Criminal Responsibility

Criminal law has two different characteristics: it deals only with individual natural persons; and it involves an element of public condemnation in the specification of criminal (Albert, 1945). International instruments suggest that state responsibility for wrongful acts and individual criminal responsibility are separate regimes of liability in nature and in form. Below, I will take a look at two different but interrelated regimes in cybercrimes.

International law

According to article 2 of the Draft article on Responsibility of States for Internationally Wrongful Acts, (2001), there is an internationally wrongful act of a State when that conducts of an action or omission:

1. Is attributable to the State under international law;
2. Constitutes a breach of an international obligation of the State[13].

Contrary to the criminal responsibility in national law, which is usually the responsibility of natural persons, international responsibility at international level refers to states as the original subjects of international law.

The Statute of the International Criminal Court, the Draft Articles on State Responsibility and the Draft Code of Crimes against Peace and Security of Mankind imply the dichotomy between international wrongful acts of states and the crimes committed by individuals.

The notion of individual criminal responsibility under international law has gradually evolved to complement that of state responsibility, but as I will try to demonstrate below only when individual criminality runs alongside a systemic pattern of criminality organized, tolerated, or acquiesced in by the state. However, absent a pattern of state criminality, individuals can incur criminal responsibility under international law without the state being directly responsible for their criminal acts when committed by its agents or representatives (Cassese & Jones, 2002).

Indeed, there are important obstacles in order to fulfil the criminal responsibility of governments. The most important of them is the legal entity of states and in particular the administrative procedure of government's responsibility (Fazlollah & Mohammad, 2017).

The resistance of the states for their sovereignty and the lack of any document in international law for the criminal responsibility of states are the main important barriers for criminal responsibility of states in contemporary international law. Therefore, it should be mentioned that criminal responsibility of the criminal acts and omissions at international level only triggers the individuals rather that the states. The main efforts of the institutional and normative regimes such as Budapest is also to recognize this dichotomy responsibility regime and encourage the states only to try to enhance their mutual cooperation against cybercrimes.

Iran's Legal System

Iranian legal system has experienced the sixth period of law making regarding criminal responsibility, and the most significant change in this process and the change is the identification of criminal liability for legal entities in articles 19 and 20 of the cyber-crime code. Article 19 states that:

> *"In the following cases, if a computer offense is committed in the name of a legal person and in the line with its interests, a legal person has the criminal responsibility:*
>
> 1. *Whenever a director of a legal person commits a cyber-crime,*
> 2. *Whenever a director orders for commission of a cybercrime and a crime occurs.*
> 3. *If one of the employees of the legal entity commits a cyber-crime with the permission or knowledge of the director or due to non-supervision of him.*
> 4. *Whenever all or part of the legal person's operation is allocated for committing a crime in cyber-space.'*[14]

And Article 20 states that the following persons are punished to the following sentences in accordance with the circumstances and conditions of the offense, in addition to a maximum of 3 to 6 times of the maximum amount of the fine, as follows:

1. *If the maximum sentence for imprisonment is up to 5 years, the temporary suspension of a legal person is from 1 month to 9 months and in the event of a repeated offense, a temporary suspension of the legal person is from 1 year to 5 years,*
2. *If the maximum sentence of imprisonment for that crime is more than 5 years imprisonment, the temporary suspension of the legal person is from 1 to 3 years and in case of repeated crimes, the legal person will be dissolved…"*

As it is clear, in Iranian legal system, contrary to international law, the criminal responsibility of the legal persons has been recognized, however, in any case, there are exceptions that prevent the assignment of criminal responsibility for cybercrime actions for legal entities as individuals such as bankruptcy and legal capacity.

CONCLUSION

There are many different types of cybercriminals that, according to the classical rules of international law and national law, only some of them could be categorized as international crimes. In this regard, it is necessary to recognize the necessary elements of specific intention (*mens rea*) and criminal commitment (actus reus) for the act.

Based on the international draft on responsibility of States for international wrongful acts (2001) only the offender is responsible for its wrongful acts. However, it seems that the principle of co-operation as a general principle of international law, could overcome the shortcomings and difficulties in fighting the cyber-crimes. Moreover, before the adoption of a universal comprehensive instrument in this regard, sharing of the national technical knowledge about cyber-crimes among States, establishment of an informing centre about cyber threats and attempting to reach consensus for definition of the main concepts, could make the international community more effective against the cyber-crimes.

This challenge could be considered from the separation of the regime of responsibility in international law and Iranian legal system. Nonetheless, in international law, it is only possible to invoke the international responsibility of states for their wrongful acts, in Iranian legal regime; the criminal responsibility of the legal entities for their cybercrimes has been recognized.

However, it seems that in absence of any authoritative criminal legal regime at national and international levels, the door is open for some changes and updates for law making in cyberspace both in national and international law. Criminalization of the specific crimes under Iranian legal system and updating the existing rules on one hand and strengthening international mechanisms in international law, and comprehensive efforts to a universal agreement on the concept and definition of the cybercrimes could solve some the cumulative challenges in this era and pave the road to an efficient opposing with cybercrimes.

ENDNOTE

1. The White House, available at http://www.whitehouse.gov/issues/foreign-policy/cybersecurity
2. This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

3. This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerised.
4. This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account
5. These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs.
6. This term has its origin in the word Trojan horse. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorised programme. The most common form of installing a Trojan is through email. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber-criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.
7. In these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password.
8. This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein.
9. Understanding cybercrime: Phenomena, challenges and legal response September 2012, op.cit.
10. Signed in 2001 and entry into force in 2004. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.
    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 co-operation. See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. (last visited on 20.10.2018)
11. https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime (last visited on 20.09.2018).
12. Of course differences in criminalization and execution may also arise due to varying levels of technical capacity of states. Spam, for example, is an issue that many developing countries would like to see criminalised, but is addressed by most developed countries as a civil or administrative matter.
13. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (last visited at 20.4.2018).
14. http://www.hsu.ac.ir/it/1390/12/03/1390-12-03-14-21-27/ (last visited at 1.10.2018).

REFERENCES

Adam, S. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists, 69*(5), 38-45.

Albert, G.D. (1945). Criminal responsibility of individuals and international law. *The University Of Chicago Law Review, 12*(4), 1-16.

Atul, J. (2005). *Cyber-crime: Issues and threats*. Gyan Publishing House.

Behzad, R., & Seyeed, N.A.M. (2014). Criminal liability in cyberspace according to the legal system of Iran. *Criminal Studies, 16*(1), 13-23.

Brenner, J. (2013). *Glass houses: Privacy, secrecy, and cyber insecurity in a transparent world*.

Cassese, P.G., & Jones, J.R.W.D. (2002). *The Rome statute of the international criminal court: A commentary*.

Cybercrime Legislation. (2012). *Understanding cybercrime: Phenomena, challenges and legal response.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Darid, S., Mousavi, M., & Ali, R. (2014). The scope of criminal liability of legal entity in the Islamic penal code. *Criminal Studies, 13*(1), 149-150.

Dieterle, D. (2013). Chinese hackers steal designs for top US Military Tech-Now What. *Cyber Arms-Computer Security*. Retrieved from http://cyberarms.wordpress.com/2013/05/29/chinesehackers-steal-designs-for-top-us-military-tech-now-what/

Fazlollah, F., & Mohammad, M. (2017). The international criminal responsibility of governments in the process of globalization. *Journal of Politics and Law, 10*(1), 264-265.

Jonathan, C.A. (2014). World of difference: The budapest convention on cybercrime and the challenges of harmonisation. *Monash University Law Review, 40*(3), 702-703.

Kamini, D. (2011). Cybercrime in the society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240-259.

Kesan, J.P., & Carol, M.H. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journal of Law and Technology, 25*(2), 415-529.

Lynn, M., & William, J. (2010). *Defending a new domain.* Retrieved from http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

Maynard, A.D. (2015). Navigating the fourth industrial revolution. *Nature Nanotechnology, 10*(12), 1005-1006.

Michael, N.S. (2014). The law of cyber warfare: Quo Vadis? *Stanford Law & Policy Review, 25*(2), 269-300.

Miriam, N. (2014). Convention on cybercrimes. *Legal Analysis, 43*(2), 187-195.

National Academy of Science and Engineering (ACATECH). (2013). *Recommendations, final report of the industrie 4.0 working group.* Frankfurt: ACATECH. Report.

Sophie, C.P. (2014). What is the scope of legal self-defence in International Law? *Jus ad bellum with a special view to new frontiers for self-defence.* Retrieved from http://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_2014/afh19-2014.pdf

Valeriano, B., & Ryan, C.M. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press Scholarship Online.

Yongxin, L., Eduardo, R.L., Fernando, D., Guilherme, B., & André, V. (2018). The impact of the fourth industrial revolution: A cross-country/region comparison. *Production, 28*(1), 1-18.