2017 FREDMUN CYPRUS

FREDMUN 2017

2ND – 5TH NOVEMBER 2017

DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE

COMMITTEE STUDY GUIDE

TABLE OF CONTENTS

WELCOMING MESSAGE BY THE BOARD

Dear delegates,

It is an honour and great pleasure to officially welcome you to FREDMUN 2017, which is going to be held on Cyprus from 2nd to 5th of November, and more specifically to the 1st Committee of the General Assembly. It is our utmost pleasure and privilege to serve you as your Board and we are looking forward to our interaction, communication and cooperation, prior and during the debates of our Committee. Our task can be characterized as challenging, since we are going to elaborate on two important contemporary issues that have to be efficiently and comprehensively dealt.

The first Topic is dealing with the challenging task of "Strengthening actions to end recruitment of child soldiers". Preventing the recruitment of children is the only possible way to limit their exploitation in war. It is also the sole way to protect them from the dangers of premature involvement in battlefields. Being exposed to military life is indisputable harmful to children and adolescents, and violates many of their fundamental rights, regardless of whether they are ever deployed in conflict. Our response should be unanimous and our work should exceed all expectations. The second Topic Area under discussion involves "Combating cyber warfare in the context of international security". Cybercrime has evolved from an emerging threat to a visible enemy posing direct impediments to all walks of life, whether it is about everyday financial transactions, or even hacking national databases for the purpose of political influence or espionage. Despite the different perspectives of international actors on the matter, an holistic approach towards the problem is deemed more urgent than ever before.As a result, the upcoming conference is going to give all of us a unique opportunity; the opportunity to combat the world's important issues, always contemplating that diplomacy, cooperation, respect for everyone,

accurate information and honest dialogue are the keys to success. Our Committee is faced with the challenging task of comprehensively dealing with two crucial and contemporary issues placed at the top of the international agenda. A decent start, shall be the review of your study guide as a stepping stone from where you can expand your research, as we urge you to thoroughly research on the Topics, study your country's policy, start brainstorming on possible solutions and proposals, as well as passionately raise your voice. Do not hesitate to contact us for your possible queries!

The Board of the DISEC Committee

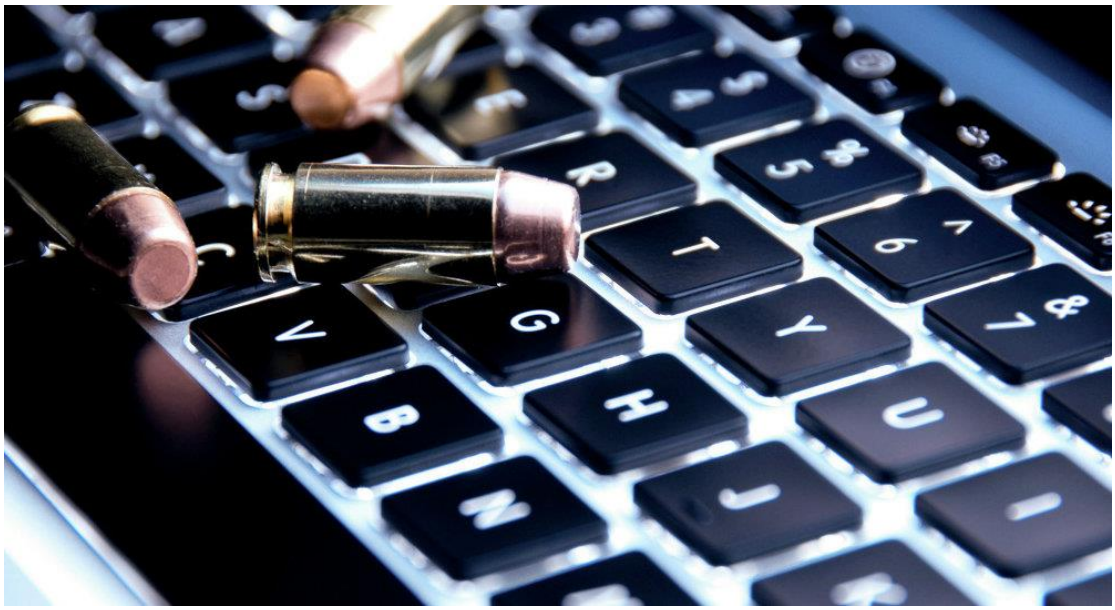
INTRODUCTION TO THE COMMITTEE

The First Committee of the General Assembly (GA) of the United Nations (UN), also known as the Disarmament and International Security (DISEC) is a committee of paramount importance for the function of the Organization. Its resolutions, in respect to the Charter of the United Nations, aim to defend "the general principles of cooperation in the maintenance of international peace and security", to promote "disarmament and the regulation of armaments" and to help with the "promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments".
These decisions are not binding for the member states in a legal sense, but serve as a common basis of understanding for cooperation among member states on the issues regarding disarmament and international security.

DISEC also convenes frequently and closely with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament.[1]

[1] UN GENERAL ASSEMBLY - FIRST COMMITTEE - DISARMAMENT AND INTERNATIONAL SECURITY, In-text: (Un.org, 2017), Your Bibliography: Un.org. (2017). UN General Assembly - First Committee - Disarmament and International Security. [online] Available at: http://www.un.org/en/ga/first/ [Accessed 10 Sep. 2017].

Topic B: Combating cyber warfare in the context of international security



Gun bullet on a laptop/Sputnik News (2016)
Available at https://sputniknews.com/military/201612021048115584-us-plan-for-cyber-unit/

INTRODUCTION TO THE TOPIC

The interconnected nature of information and communication technologies (ICTs) in the 21st century, has caused an unprecedented erosion in the online borders, making cyber security a transnational issue, which is to be dealt via a global approach.
Cybercrime and cyber warfare are becoming more and more organized, costing more than a trillion dollars per year in practices that include inter alia, identity theft, online fraud and loss of intellectual property, targeting millions of people worldwide, as well as businesses and national governments.

In the spirit of combating the emerging threat of cybercrime, the United Nations Economic and Social Council (ECOSOC), launched a special event on the 9th of December 2011, in New York, raising the issue of "Cybersecurity and Development"[2]. The discussions were concentrated in three specific pillars:

(1) Awareness building concerning the ongoing situation, the emerging challenges of cybersecurity and its ties to development,

(2) The identification of the best practices and policies in the direction of forming a solid background of cybersecurity globally,

(3) The further research for options and strategies in the purpose of shaping a holistic approach towards the rising threat of cyber warfare.

The question of whether a cybercriminal activity is perpetrated by a state or a Non-State Actor (NSA) is challenging and in many cases, remains unanswered. That's exactly the reason why tackling this issue demands the cooperation not only among states but between the states and the private sector, as well. Furthermore, mobilizing the civil society is of utmost importance, while maintain close cooperation with law enforcement agencies.

A useful metaphor to further understand the interconnectivity of cyber security is to think of it as the financial and banking interconnectivity of the states. As it has been proven by the economic crisis of 2008, taking a step back in a national economy can create a domino effect with tremendously extended repercussions.

The nature and the proceedings of cybersecurity and by extend of cyberwarfare, is in most cases not available to the public. Of course, one should not overlook the socio-economic factor of the topic under discussion; the division between the developed and developing states. The developing world often may not have

[2] CYBERSECURITY: A GLOBAL ISSUE DEMANDING A GLOBAL APPROACH | UN DESA | UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, In-text: (Un.org, 2017), Your Bibliography: Un.org. (2017). Cybersecurity: A global issue demanding a global approach | UN DESA | United Nations Department of Economic and Social Affairs. [online] Available at: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html [Accessed 10 Sep. 2017].

the demanded economic and technological resources to combat cybercrime and effectively contribute to the safeguarding of cyber peace. This situation creates the ideal circumstances for a "safe haven" for cybercrime perpetrators as it creates a window of opportunity for them, full of legal loopholes and technical deficiency.

High risks are also being faced by underage users. Communities as well as families have to provide young people, entering the cyber world for the first time with the appropriate instructions, and of course, cautionary remarks. More specifically, media literacy guidelines provided online by International Telecommunications Union (ITU)[3] are of imperative importance for the above purpose.

The legal cornerstone concerning the combating of cybercrime is the Budapest Convention. In brief, this international treaty holds as its primordial goal the harmonization of national criminal legislative measures for the prosecution of cybercrimes including but not limited to; copyright infringement, fraud, child pornography, hate crimes and breaches of network security.

In this regard, efforts are being made in building upon the Budapest Convention (2001, *Convention on Cybercrime*)[4] through enhancing it with the introduction of a global strategy.

Taking into consideration all of the abovementioned factors, it can be concluded that the global aspect of the problem is consistently underlined by the states and points to the direction of global partnership as its solution.

The United Nations are committed to employ their full strategic and analytic capabilities to their full extent in order to efficiently and effectively combat this burning issue for the international community.[5]

DEFINITION OF KEY TERMS

It is imperative that certain terms both general and technical are explicitly defined and explained at this point so as to facilitate you with your research and understanding of the topic. Bear in mind that for more general terms often there is more than one accepted definition.

---

[3] PRESS RELEASE: GUIDELINES PROPOSED FOR CHILD ONLINE PROTECTION (COP) INITIATIVE, In-text: (Itu.int, 2017), Your Bibliography: Itu.int. (2017). Press release: Guidelines proposed for Child Online Protection (COP) initiative. [online] Available at: http://www.itu.int/newsroom/press_releases/2009/14.html [Accessed 10 Sep. 2017].

[4] CONVENTION, B. AND EUROPE, C., Budapest Convention and related standards, In-text: (Convention and Europe, 2017), Your Bibliography: Convention, B. and Europe, C. (2017). Budapest Convention and related standards. [online] Cybercrime. Available at: http://www.coe.int/en/web/cybercrime/the-budapest-convention [Accessed 10 Sep. 2017].

[5] PRESS RELEASE: GUIDELINES PROPOSED FOR CHILD ONLINE PROTECTION (COP) INITIATIVE, In-text: (Itu.int, 2017), Your Bibliography: Itu.int. (2017). Press release: Guidelines proposed for Child Online Protection (COP) initiative. [online] Available at: http://www.itu.int/newsroom/press_releases/2009/14.html [Accessed 10 Sep. 2017].

International security

Generally refers to the synthesis of measures adopted by governmental and intergovernmental authorities for the purpose of ensuring *survival* and *safety*. These measures vary and can escalate from diplomatic agreements to military action. Undoubtedly, international and national security are directly linked and some might say that one works are a prerequisite for the other.[6]

Cybercrime

Cybercrime is a criminal act and can be defined as "an offence that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)"[7]

As underlined by the Budapest Convention (2001) some terms related to the technical nature of a cybercrime have to be further explained, and explicitly defined;

a. *"computer system"* means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b. *"computer data"* means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c. *"service provider"* means:
    i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
    ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
d. *"traffic data"* means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[8]

---

[6] BUZAN, B. AND HANSEN, L. The evolution of international security studies, In-text: (Buzan and Hansen, 2015), Your Bibliography: Buzan, B. and Hansen, L. (2015). The evolution of international security studies. Cambridge: Cambridge University Press.
[7] HALDER, D. AND JAISHANKAR, K. Cyber crime and the victimization of women,, In-text: (Halder and Jaishankar, 2012), Your Bibliography: Halder, D. and Jaishankar, K. (2012). Cyber crime and the victimization of women. Hershey, PA: Information Science Reference.
[8] CITE A WEBSITE - CITE THIS FOR ME, In-text: (Rm.coe.int, 2017), Your Bibliography: Rm.coe.int. (2017). Cite a Website - Cite This For Me. [online] Available at: https://rm.coe.int/16806f9471 [Accessed 10 Sep. 2017].

Cyberwarfare

Defined as any virtual act of aggression with a political motivation aiming to affect the enemy's computer and information systems. The ultimate goal is to paralyze the financial and organizational systems via means of alternation or theft of top secret information, thus undermining and rendering useless networks, important websites and essential services.

There are 2 possible acts of virtual aggression:

i. *Sabotage* the end goal is to disrupt the flow of operations and equipment necessary for the military and financial computer systems to function properly such as but not limited to; communications, fuel, power and transportation infrastructures.

ii. *Espionage and/or security breaches* the theft and unlawful acquisition of classified information from the enemy's institutions for purposes of military, political or financial nature. The method used is the disabling of the rival's networks, software, computers or the Internet.[9]

Cybersecurity

Cybersecurity[10] is the safeguarding of an online system's security, an online database's intactness and overall, the maintenance of one's virtual "sovereignty". To safeguard the above methods of prevention are of utmost importance. One to protect themselves has to have a comprehensive and in-depth understanding of the enemy's "arsenal" as well as possible strategies. This translates to having a knowledge upon the potential information threats, such as an advanced virtual "virus" or other malicious programs. Cybersecurity defense strategies are largely based upon;

i. Identity management,
ii. Risk management
iii. Incident management

Denial-of-Service Attack (DoS)

"A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service." In a DoS attack, the hacker usually sends a plethora of messages asking the server or network to

[9] WHAT IS CYBERWARFARE (CYBER WAR)? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is Cyberwarfare (Cyber War)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/13600/cyberwarfare [Accessed 10 Sep. 2017].

[10] WHAT IS CYBERSECURITY? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is Cybersecurity? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24747/cybersecurity [Accessed 10 Sep. 2017].

authenticate requests whose return addresses are invalid. The server or network, unable to find the return address of the perpetrator when sending the authentication approval, causes the server to wait before termination of the connection. When the network closes the connection, the hacker sends more authentication messages whose return addresses are also invalid. This results in the restart of the authentication process, keeping the network or server busy.

DoS attacks can cause ineffective or inaccessible services, connection interference or even interruption of network traffic.[11]

Computer Emergency Response Team (CERT)

"A computer emergency response team (CERT) is a group of experts who respond to cybersecurity incidents." In general, the designation of CERT aims to confront the evolution of viruses, malware as well as other cyber-attacks, via the application of real-world solutions to these problems. They may be associated with government or work as employees of a major corporation. For instance, the U.S. Computer Emergency Readiness Team (US-CERT) operates under the U.S. Department of Homeland Security.[12]

HISTORY OF THE TOPIC

Over the past decades, the impact and scale of cyber-attacks has developed in an unprecedented rate. As cybercrime gets more and more sophisticated, so has the cybersecurity against it. Some examples of this twofold evolution will be examined above, in the purpose of enlightening the threat landscape and the security response progression over the years.

Computer Worms (Late 1980s-Early 1990s)

The first computer worm was created by Robert Morris in 1989. Aggressively and rapidly spread, this self-propagating virus managed to severely obstruct internet services. The Morris worm was a significant incident, interpreted as the first ever widespread example of denial-of-service (DoS) attack. However, internet back in late 1980s was in its very early stages, making the impact of Morris worms nearly insignificant comparing to the devastating consequences they would have today.

---

[11] WHAT IS A DENIAL-OF-SERVICE ATTACK (DOS)? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is a Denial-of-Service Attack (DoS)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24841/denial-of-service-attack-dos [Accessed 10 Sep. 2017].

[12] WHAT IS A COMPUTER EMERGENCY RESPONSE TEAM (CERT)? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is a Computer Emergency Response Team (CERT)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert [Accessed 10 Sep. 2017].

Despite the limited threat, the first computer worms set the foundation for the nuisance of the cyber security industry. Initially, the industry reacted according to the well-known saying "prevention is better than a cure", supporting the primordial role of detective security and preventative manufactured products. A cornerstone in the progress of the cyber security industry, was the establishment of CERTs (Computer Emergency Response Teams), taking up the role of a central coordinator in anti-cybercrime emergency responses, in the direction of achieving a holistic and more efficient approach.[13]

The emergence of the first viruses (1990s)

The next decade brought an important increase in internet users, consecutively expanding the risks and challenges in cyber space. New threats, called "viruses" went viral and dominated cyber warfare. Instances such as the Melissa[14] and the ILOVEYOU[15] virus brought about the infection of millions of PCs, causing the failure of email systems world-wide, all conducted under the scope of servicing strategic and financial interests. Antivirus technology was developed as a response to these threats, targeting the viruses' signatures and hindering them from executing. Additionally, these attacks marked the starting point of the awareness raising process in terms of opening emails from untrusted or unverified sources. This phenomenon was more evident in several companies due to the ability of viruses to spread among corporate email accounts and bring into public eye questions about the security and the uprightness of the company.[16]

Credit card attack (Late 2000s)

During the millennium decade cyber-attacks changed radically, becoming more target-oriented. Between 2005 and 2007, the first serial data violation of credit card numbers took place. The mastermind behind this previously unheard fraud was Albert Gonzalez, who created a criminal ring that enabled him to steal information from approximately 45.7 million payment cards. The card holders

---

[13] JULIAN, T., Defining Moments in the History of Cyber-Security, In-text: (Julian, 2017), Your Bibliography: Julian, T. (2017). Defining Moments in the History of Cyber-Security. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/ [Accessed 10 Sep. 2017].

[14] THE MOST FAMOUS VIRUS HISTORY: MELISSA.A - PANDA SECURITY MEDIACENTER, In-text: (Panda Security Mediacenter, 2017), Your Bibliography: Panda Security Mediacenter. (2017). The Most Famous Virus History: Melissa.A - Panda Security Mediacenter. [online] Available at: http://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/ [Accessed 10 Sep. 2017].

[15] LOVEBUG SET STAGE FOR CYBERCRIME, In-text: (BBC News, 2017), Your Bibliography: BBC News. (2017). Lovebug set stage for cybercrime. [online] Available at: http://www.bbc.com/news/10095957 [Accessed 10 Sep. 2017].

[16] JULIAN, T., Defining Moments in the History of Cyber-Security, In-text: (Julian, 2017), Your Bibliography: Julian, T. (2017). Defining Moments in the History of Cyber-Security. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/ [Accessed 10 Sep. 2017].

were customers of US retailer TJX, costing the company more than $256 million.[17]

This massive security compromise made matters more serious, as enterprises found out the hard way the dreadful consequences of being exposed to threats and started to arm themselves with state-of-the-art security systems adapted to new reality challenges.

The Threat Tsunami and the Target Breach (Nowadays)

Target breach is a process in which the perpetrators are able to lift "track data", enabling them to manufacture and sell counterfeit cards. 40 million of debit and credit cards were stolen via this scam, causing severe turbulences to the existing cyber security practices.[18]

The perpetrators used an indirect route, via a third party, by hacking into point-of-sale (PoS) systems, using a specifically developed code, grabbing decrypted credit card numbers. This incident made cybercrime a matter of public response, rendering ineffective the ad hoc approaches by companies and pointing out the necessity of the adoption of a holistic strategy towards the issue.

The future of anti-cybercrime response

Admittedly, the sophistication of cybercrime makes it truly difficult to prevent. Organizations should emphasize on how to hinder a possible spread of the breach and construct solid post-crisis management strategies in the purpose of controlling the aftermath and responding to it efficiently. Building organizational resilience is a key factor in alleviating the "pain" caused by cyber threats in every aspect of their existence.

LEGAL FRAMEWORK

As previously mentioned, many efforts have already been made on creating substantive and enduring documents to promote the partnership and cooperation among states upon the matter of ensuring cybersecurity for all. Regional organizations as well as international ones have drafted and signed documents, but due to a plethora of circumstantial challenges (e.g. the technological divide), their implementation is far from achievable. In any case,

[17] TJX CARD FRAUD MASTERMIND JAILED FOR 20 YEARS, In-text: (Infosecurity Magazine, 2017), Your Bibliography: Infosecurity Magazine. (2017). TJX card fraud mastermind jailed for 20 years. [online] Available at: https://www.infosecurity-magazine.com/news/tjx-card-fraud-mastermind-jailed-for-20-years/ [Accessed 10 Sep. 2017].

[18] OB, T., Target Breach Affecting 40 Million Was Likely an Inside Job, In-text: (Job, 2017), Your Bibliography: Job, T. (2017). Target Breach Affecting 40 Million Was Likely an Inside Job. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/target-breach-affecting-40-million-was-likely-an/ [Accessed 10 Sep. 2017].

legal framework will be the legal basis of your research that will guide you through out the topic, your statements and ideas should always follow the international conventions and treaties.

E.U. Legislation on Combating Cybercrime

For the purposes of further understanding what an effective and efficient legal framework on combating cybercrime requires, it is useful to examine European legislation upon the matter. The E.U. may well be a regional organization, but it is still centered on international understanding and cooperation, thus it shall work as an effective paradigm for the challenges and the demands the creation of a global partnership agreement might bring about.

Briefly, the main goals (that also reflect the implementation challenges) that the European legislative endeavor tries to achieve are the following ones: [19]

i. ***reduction of frictions among national legislations***
This is a common issue that arises within the European Union state-parties regarding many legislative areas that require joined actions. However, this may be met in other international efforts, as well. Usually, one may find non legal factors behind this frictions for instance; national security protection claims, politics and internal social idiosyncrasies, the economy and the public opinion of the people.

ii. ***the introduction of new investigative powers***
The question of giving away a part of a state's sovereignty for security is an ever-lasting one for the international political scene. Thus, the endeavor is challenging and might come across many skeptics from many different states.

iii. ***the facilitation of international cooperation***
States are plagued by constant security dilemmas that used to refer to military insecurity, but have since developed to include from information safeguarding to environmental security issues. Despite their cooperation in many fields, states (even within the E.U.) may perceive another nation's action as a threat direct or indirect to their survival. This situation is translated –in the best case scenario- as a hesitation towards international cooperation upon substantial issues such as; information sharing.

[19] CYBERCRIME - MIGRATION AND HOME AFFAIRS - EUROPEAN COMMISSION, In-text: (Migration and Home Affairs - European Commission, 2017), Your Bibliography: Migration and Home Affairs - European Commission. (2017). Cybercrime - Migration and Home Affairs - European Commission. [online] Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en [Accessed 10 Sep. 2017].

More specifically, within the European legal context, two international agreements are the most prevalent both for their (primarily) European focus and their legal impact:

- the ***2001 Council of Europe Convention on Cybercrime*** [20](Budapest Convention) and
- the ***2005 European Union Framework Decision on attacks against information systems***[21] (Council of Europe, 2001; European Union, 2005)

Asia –Pacific Legislation on Combating Cybercrime

Following to an Asia-Pacific Economic Cooperation (APEC) Heads of States meeting in October 2002, the leaders decided upon 3 (similar to the E.U.'s) goals; i) the creation of a common legal framework (not requiring the European harmonization), ii) law enforcement investigation units (less "invasive" for the states than the investigative powers of the E.U.) and iii) the CERT network.

More specifically, it was stated that their aim was the*"Endeavor to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)."*

The Ministers decided upon a Comprehensive APEC Strategy (2002) that would entail;

- Legal Developments
- Information Sharing
- Security and Technical Guidelines
- Training and Education
- Wireless and Emerging Technologies

Also, great importance was given to the socio-economic (and by association technological) divide; *"Thus, the fight against cybercrime and the protection of critical infrastructures is built upon the legal frameworks of every economy."*

---

[20]ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 10 Sep. 2017].

[21] EUR-LEX - L33193 - EN - EUR-LEX, In-text: (Eur-lex.europa.eu, 2017), Your Bibliography: Eur-lex.europa.eu. (2017). EUR-Lex - l33193 - EN - EUR-Lex. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Al33193 [Accessed 10 Sep. 2017].

The APEC states, determined to address effectively the issue, engaged in a multitude of cybercrime legislation projects, including but not limited to; questions upon the existing conventions (mainly the Convention on Cybercrime (2001) of Budapest) and drafting procedures. Furthermore, a series of conferences for cybercrime experts was held in Bangkok (July 2003), Hanoi (September 2004) Seoul (June 2005), when the specifics of drafting cybercriminal laws were discussed, the improvement of cybercrime investigation was stressed and of course, the amelioration of international cooperation on the matter. What is more, direct assistance projects were introduced with consultations on exchange of cybercrime legislation expertise and experience and to address the arising issue of hesitation and uncertainty, the possibility for confidential analysis of draft laws.

Some of the most notable actions towards creating a legal framework for the area are the following;

- **Philippines, January 2004**
  – Training for 60 legislative staff
  – Direct assistance to law drafters

- **Indonesia, March 2004**
  – Training for law makers, ministry of information, law enforcement, academia and business
  – Developed plan to draft and enact cybercrime provisions

- **Vietnam, August 2004**
  – Training for law makers, ministry of post and telematics, ministry of justice, prosecutors
  – Meetings with high-level officials to discuss legislative options

International Legislation on Combating Cybercrime[22]

Budapest Convention[23]

The *2001 Council of Europe Convention on Cybercrime* (Budapest Convention) is largely and frequently used as the basis of discussion both in regional cooperation and when the discussing the prospect of a new international legal framework. It is the point of reference for every issue related

[22] CITE A WEBSITE - CITE THIS FOR ME, In-text: (Ssoar.info, 2017), Your Bibliography: Ssoar.info. (2017). Cite a Website - Cite This For Me. [online] Available at: http://www.ssoar.info/ssoar/bitstream/handle/document/27731/ssoar-clsc-2010-5-calderoni-the_european_legal_framework_on.pdf?sequence=1 [Accessed 10 Sep. 2017].
[23] ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 10 Sep. 2017].

to international cybersecurity and the main instrument regarding its combating.

Harmonization of the state-parties domestic national laws, improvement of the global investigation of cybercrime and assorted techniques that are to be followed in these cases, as well as realization of a truly international cooperation amongst states constitute the main goals of the Convention.

The ratification of this convention has been concluded by the majority of E.U. states, the United States of America, Japan, Australia and Canada.

As a result, the EU's law enforcement agency, Europol, and its Joint Cybercrime Action Taskforce, cooperate when it comes to cybercrime investigation procedures. In addition, INTERPOL is helping in coordinating efforts between states by supporting national police, facilitating information exchange and providing updates on investigations.

Nevertheless, influential countries, such as Russia, China and India have not ratified the document.

DISCUSSION OF THE TOPIC

First and foremost, there is a need to keep an equilibrium between the privacy of citizens (and states) and public safety (and consequently, cybersecurity). Privacy is a primordial human right. "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence…" (Art. XII, Universal Declaration of Human Rights). Respect for privacy is the cornerstone of democracy, because it is directly linked to free thought and expression. However, privacy of computer networks is just as important as it includes many times sensitive personal data. Thus, the need for investigation of such crimes arises now more than ever.

Moreover, cross border coordination is essential to the modern globalized nature of cybercrime, and the international legal framework needs to correspond to this circumstance. When a threat is global (e.g. "wannacry" malware that hit at the same time 150 states), the procedure of investigating the perpetrators needs to be global to be efficient. Thus, a complex international investigation is required. However, as it has been already stated, legal framework for cooperation on the matter is rather lacking and mainly focuses upon regional cooperation, while it gives no one single investigative governance authority. As a result, the investigation process is rendered tremendously complicated and eventually, ineffective.

Even in cases where the perpetrator of such acts of aggression is found, there is the possibility that they have fled to a "safe haven", where cybercrime laws are largely ineffective (or non-existent) and implementing an extradition request is essentially unachievable.

What is more, jurisdictional limitations are definitely a deterrent to the speed with which a global evidence gathering process moves. With cross-border investigations, a law enforcement agency is required to go through a multitude of bureaucratic procedures that can take up more than valuable time. Electronic evidence is even more difficult to detect and even easier to hide. Of course, to this regard, the private sector can surpass some of these jurisdictional procedures and provide access to evidence held by private industry. Nevertheless, this does not mean that a need for an international effective understanding brought by a global cooperation framework is not still imperative.

All in all, it should be underlined that the Budapest Convention of 2001, which is currently the most prevalent international convention on the matter, is highly effective given the circumstances and the fact that it was signed 16 years ago. The harmonization of domestic laws by its state parties is largely achieved and non-state parties have been using it as a model for their cybercrime legislation, as well.

Thus, the question that comes forward is that the international community should not waste this stable ground put forward by this treaty and should instead build upon it by discussing with the non-members their hesitations. After all, is it the Budapest Convention really an international one if such a large amount of countries are not included?[24]

BLOC POSITIONS

European Union

Cybercrime is a priority for the mandate of the European Commission in the field of security. Given the constant increase in reliance on online services, the cost of cyber-attacks to European Union's economy has grown in an unprecedented rate. This new challenge has brought about the need for an extensive harmonization of domestic legal framework, hence the issue of the

[24] BUILDING A STRONGER INTERNATIONAL LEGAL FRAMEWORK ON CYBERCRIME, In-text: (Chatham House, 2017), Your Bibliography: Chatham House. (2017). Building a Stronger International Legal Framework on Cybercrime. [online] Available at: https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime [Accessed 10 Sep. 2017].

Directive on Attacks against Information Systems[25], enhancing the cooperation between public authorities on the one hand, and the private sector and civil society on the other. EUROPOL meets the burden of investigation on cyber-attacks, conducting thorough analyses and reports on cyber crimes in cooperation with the European Union Agency for Network and Information Security (ENISA).

Overall, European strategy towards cyber security aims to increase cyber security and cooperation, also concentrates on making the EU a stronger player in the field of cybersecurity and mainstreaming cybersecurity in EU policies, supporting new initiatives with regard to new technologies, hence the support to the Budapest convention and its further development.[26]

U.S.A.

The main missions towards the achievement of the US strategic goals for cyber security are taken on by the Department of Defence (DoD) with a view to build and maintain ready forces and capabilities to conduct cyberspace operations, to defend and secure the DoD information network and data, as well as to mitigate risks to DoD missions. The US strategy is focused on maintaining and defending the US homeland and US vital interests from destructive or disruptive cyber-attacks of significant consequence. What is more, building and maintaining viable cyber options in the direction of controlling conflict escalation and shaping the conflict environment at all stages, is a primordial goal for the US cybersecurity strategy. Lastly, the United States support the Budapest convention and its further development in the spirit of creating robust international alliances and partnerships for the deterrence of shared threats and the increase of international security and stability.[27]

Russian Federation

The Russian Federation remains reluctant on cooperation relationship with EU states on cybercrime, with a major sticking point in promoting cybersecurity cooperation between Russia and Western countries being the difference in focus on what is under attack and what is to be secured. Hence the rejection of the Russian suggestion for a global treaty on cyber crime, by the Western block, claiming that Budapest Convention is a good basis. Promoting actively a

[25] EUR-LEX - 32013L0040 - EN - EUR-LEX, In-text: (Eur-lex.europa.eu, 2017), Your Bibliography: Eur-lex.europa.eu. (2017). EUR-Lex - 32013L0040 - EN - EUR-Lex. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1440771959763&uri=CELEX:32013L0040 [Accessed 10 Sep. 2017].
[26] CYBERSECURITY, In-text: (Digital Single Market, 2017), Your Bibliography: Digital Single Market. (2017). Cybersecurity. [online] Available at: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity [Accessed 10 Sep. 2017].
[27] ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Accessed 10 Sep. 2017].

proposal for a UN global treaty on cybercrime, the Russian Federation is pursuing to solve the problem of attribution of cyber-attacks, enhance the ability of the international system to address cyber crimes, opting for a symmetrical retaliation response, avoiding the further escalation that may involve non-cyber tools.

All in all, Russian perspective on cyber warfare consists of three pillars; i) countering cybercrime, ii) information sharing, iii) addressing the issue of global Internet governance. To achieve all of the above, diplomatic, policy, and political efforts are critical, while cooperation is also needed at a more technical level.[28]

Peoples' Republic of China

The release of the first National Cybersecurity Strategy by the Cyberspace Administration of China (CAC), illustrates and reaffirms China's main positions on the development and security of cyberspace. The strategy intends to build China into a cyber power, setting as a primordial goal the protection of the "new territory of sovereignty".

With a view to accomplishing the aforementioned strategy, the major task include inter alia the protection of national security and critical information infrastructure, the building of a healthy online culture, the improvement of cyber governance, the enhancement of baseline cybersecurity, the elevation of cyberspace defense capabilities and the strengthening of international cooperation via the endorsement of UN initiatives in cyberspace.[29]

ACTIONS THAT HAVE ALREADY BEEN TAKEN

GA resolution 65/230

This resolution emphasizes upon the establishment of an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation and best practices towards cyber threats and the possible means for their confrontation, the exchange of know-how capacity and

[28] ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: http://russiancouncil.ru/papers/RIAC-EWI-Russia-US-Cybersecurity-Policybrief11-en.pdf [Accessed 10 Sep. 2017].
[29] CHINA PUBLISHES FIRST NATIONAL CYBERSECURITY STRATEGY, In-text: (Usito.org, 2017), Your Bibliography: Usito.org. (2017). China Publishes First National Cybersecurity Strategy. [online] Available at: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy [Accessed 10 Sep. 2017].

technical assistance among member states and the promotion of international cooperation in the spirit of achieving a comprehensive approach towards cybercrime.

In addition, this resolution is a useful guide serving as an important tool to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.[30]

ECOSOC resolution 2011/13[31]

This called for a UNODC study on the effects of new information technologies on the abuse and exploitation of children. Although, this does not constitute a cybercrime in the political sense, it is still the use of virtual means for perpetrating criminal actions. This resolution is a valuable asset for understanding the repercussions of new information technologies in everyday life as it provides a thorough identification and description and evaluation of the problem, proposing specific measures for its confrontation and presenting opportunities to upgrade the fight against ICT-facilitated child abuse and exploitation.

United Nations Office on Drugs and Crime (UNODC) Global Program on Cybercrime[32]

Valuable technical assistance for different groups is provided: policy-makers and legislators; criminal justice and law enforcement personnel; central authorities is also given by the United Nations Office on Drugs and Crime. Targeting the regions of Central America, Eastern Africa and Southeast Asia the program is thematically focused on Digital Forensics, Cybercrime and Human Rights, via the launch of regional training for law enforcement, prosecutors and judges, the organization of national workshops on cybercrime and the conduction of country assessments concerning their response to cybercrime.

[30] TEAM, O. ODS HOME PAGE, In-text: (Team, 2017), Your Bibliography: Team, O. (2017). ODS HOME PAGE. [online] Documents-dds-ny.un.org. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement [Accessed 10 Sep. 2017].
[31] ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: https://www.unodc.org/documents/organized- crime/cybercrime/Study_on_the_Effects.pdf [Accessed 10 Sep. 2017].
[32] ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: https://www.oas.org/juridico/PDFs/cyb9_unodc_Dec16_v1.pdf [Accessed 10 Sep. 2017].

QUESTIONS TO BE ADDRESSED – POINTS A RESOLUTION SHOULD ADDRESS

- Should states discuss upon the Budapest Convention or proceed with creating a new one on ground zero?
- Which is the middle ground solution between the safeguard of privacy and the protection of the citizens?
- Is cross border coordination in global investigation procedures delayed by bureaucratic procedures? If so, how can that change?
- How can technological and cybercriminal "safe haven" states be diminished?
- How can the effective exchange of knowledge, technical know-how and best practices be efficiently achieved?
- What measures need to be taken in order to enhance the international cyberspace defense capabilities?
- How can symmetrical response towards cyber crime be achieved in the purpose of avoiding the escalation with non-cyber tools?
- Which shall be the contribution of national security services in the cross border efforts for the improvement of cyber governance?

CONCLUSION

In conclusion, the issue of cybersecurity is of utmost importance given the current circumstances of our globalized immensely interconnected world. The task of safeguarding international security for the international community is paradoxically enough an issue pertaining to the national security of each state. The result is the essential need to develop real, efficient and effective international cooperation on the matter, in accordance with the already existing international legal framework, or even the further creation of the proper legislative tools to fight the emerging threat of cyber warfare.

However, is that need met? Unfortunately, only partially. Regional cooperation is quite active on the matter, but the nature of this problem requests for a global response, and more specifically, a global framework on cooperation. Bloc positions may differ, but they all consist of the same bottom-line goal, the prevention of cyber crimes. The question that arises is how these minor differences can be set aside in the direction of accomplishing a holistic approach in a cross border issue, such as cybercrime. The engagement into a close cooperation with government, business and civil society leaders from around the world is needed more than ever in order to seek for a conflict reduction and the promotion of stability, innovation and inclusion in cyberspace.

Budapest Convention constitutes an excellent basis, but it is outdated and not universally accepted and followed. At the same time, threats of nowadays international society are imminent.

BIBLIOGRAPHY

- UN GENERAL ASSEMBLY - FIRST COMMITTEE - DISARMAMENT AND INTERNATIONAL SECURITY, In-text: (Un.org, 2017), Your Bibliography: Un.org. (2017). UN General Assembly - First Committee - Disarmament and International Security. [online] Available at: http://www.un.org/en/ga/first/ [Accessed 10 Sep. 2017].
- CYBERSECURITY: A GLOBAL ISSUE DEMANDING A GLOBAL APPROACH | UN DESA | UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, In-text: (Un.org, 2017), Your Bibliography: Un.org. (2017). Cybersecurity: A global issue demanding a global approach | UN DESA | United Nations Department of Economic and Social Affairs. [online] Available at: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html [Accessed 10 Sep. 2017].
- PRESS RELEASE: GUIDELINES PROPOSED FOR CHILD ONLINE PROTECTION (COP) INITIATIVE, In-text: (Itu.int, 2017), Your Bibliography: Itu.int. (2017). Press release: Guidelines proposed for Child Online Protection (COP) initiative. [online] Available at: http://www.itu.int/newsroom/press_releases/2009/14.html [Accessed 10 Sep. 2017].
- CONVENTION, B. AND EUROPE, C., Budapest Convention and related standards, In-text: (Convention and Europe, 2017), Your Bibliography: Convention, B. and Europe, C. (2017). Budapest Convention and related standards. [online] Cybercrime. Available at: http://www.coe.int/en/web/cybercrime/the-budapest-convention [Accessed 10 Sep. 2017].
- PRESS RELEASE: GUIDELINES PROPOSED FOR CHILD ONLINE PROTECTION (COP) INITIATIVE, In-text: (Itu.int, 2017), Your Bibliography: Itu.int. (2017). Press release: Guidelines proposed for Child Online Protection (COP) initiative. [online] Available at: http://www.itu.int/newsroom/press_releases/2009/14.html [Accessed 10 Sep. 2017]
- BUZAN, B. AND HANSEN, L. The evolution of international security studies, In-text: (Buzan and Hansen, 2015), Your Bibliography: Buzan, B. and Hansen, L. (2015). The evolution of international security studies. Cambridge: Cambridge University Press.
- HALDER, D. AND JAISHANKAR, K. Cyber crime and the victimization of women,, In-text: (Halder and Jaishankar, 2012), Your Bibliography:

Halder, D. and Jaishankar, K. (2012). Cyber crime and the victimization of women. Hershey, PA: Information Science Reference.

- CITE A WEBSITE - CITE THIS FOR ME, In-text: (Rm.coe.int, 2017), Your Bibliography: Rm.coe.int. (2017). Cite a Website - Cite This For Me. [online] Available at: https://rm.coe.int/16806f9471 [Accessed 10 Sep. 2017].
- WHAT IS CYBERWARFARE (CYBER WAR)? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is Cyberwarfare (Cyber War)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/13600/cyberwarfare [Accessed 10 Sep. 2017].
- WHAT IS CYBERSECURITY? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is Cybersecurity? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24747/cybersecurity [Accessed 10 Sep. 2017].
- WHAT IS A DENIAL-OF-SERVICE ATTACK (DOS)? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is a Denial-of-Service Attack (DoS)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24841/denial-of-service-attack-dos [Accessed 10 Sep. 2017].
- WHAT IS A COMPUTER EMERGENCY RESPONSE TEAM (CERT)? - DEFINITION FROM TECHOPEDIA, In-text: (Techopedia.com, 2017), Your Bibliography: Techopedia.com. (2017). What is a Computer Emergency Response Team (CERT)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert [Accessed 10 Sep. 2017].
- JULIAN, T., Defining Moments in the History of Cyber-Security, In-text: (Julian, 2017), Your Bibliography: Julian, T. (2017). Defining Moments in the History of Cyber-Security. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/ [Accessed 10 Sep. 2017].
- THE MOST FAMOUS VIRUS HISTORY: MELISSA.A - PANDA SECURITY MEDIACENTER, In-text: (Panda Security Mediacenter, 2017), Your Bibliography: Panda Security Mediacenter. (2017). The Most Famous Virus History: Melissa.A - Panda Security Mediacenter. [online] Available at: http://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/ [Accessed 10 Sep. 2017].
- LOVEBUG SET STAGE FOR CYBERCRIME, In-text: (BBC News, 2017),

Your Bibliography: BBC News. (2017). Lovebug set stage for cybercrime. [online] Available at: http://www.bbc.com/news/10095957 [Accessed 10 Sep. 2017].

- JULIAN, T., Defining Moments in the History of Cyber-Security, In-text: (Julian, 2017), Your Bibliography: Julian, T. (2017). Defining Moments in the History of Cyber-Security. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/ [Accessed 10 Sep. 2017].
- TJX CARD FRAUD MASTERMIND JAILED FOR 20 YEARS, In-text: (Infosecurity Magazine, 2017), Your Bibliography: Infosecurity Magazine. (2017). TJX card fraud mastermind jailed for 20 years. [online] Available at: https://www.infosecurity-magazine.com/news/tjx-card-fraud-mastermind-jailed-for-20-years/ [Accessed 10 Sep. 2017].
- OB, T., Target Breach Affecting 40 Million Was Likely an Inside Job, In-text: (Job, 2017), Your Bibliography: Job, T. (2017). Target Breach Affecting 40 Million Was Likely an Inside Job. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/target-breach-affecting-40-million-was-likely-an/ [Accessed 10 Sep. 2017].
- CYBERCRIME - MIGRATION AND HOME AFFAIRS - EUROPEAN COMMISSION, In-text: (Migration and Home Affairs - European Commission, 2017), Your Bibliography: Migration and Home Affairs - European Commission. (2017). Cybercrime - Migration and Home Affairs - European Commission. [online] Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en [Accessed 10 Sep. 2017].
- ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 10 Sep. 2017].
- EUR-LEX - L33193 - EN - EUR-LEX, In-text: (Eur-lex.europa.eu, 2017), Your Bibliography: Eur-lex.europa.eu. (2017). EUR-Lex - l33193 - EN - EUR-Lex. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Al33193 [Accessed 10 Sep. 2017].
- CITE A WEBSITE - CITE THIS FOR ME, In-text: (Ssoar.info, 2017), Your Bibliography: Ssoar.info. (2017). Cite a Website - Cite This For Me. [online] Available at: http://www.ssoar.info/ssoar/bitstream/handle/document/27731/ssoar-clsc-2010-5-calderoni-the_european_legal_framework_on.pdf?sequence=1 [Accessed 10 Sep. 2017].
- TEAM, O. ODS HOME PAGE, In-text: (Team, 2017), Your Bibliography:

Team, O. (2017). ODS HOME PAGE. [online] Documents-dds-ny.un.org. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement [Accessed 10 Sep. 2017].

- ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf [Accessed 10 Sep. 2017].
- ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: https://www.oas.org/juridico/PDFs/cyb9_unodc_Dec16_v1.pdf [Accessed 10 Sep. 2017].
- ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 10 Sep. 2017].
- BUILDING A STRONGER INTERNATIONAL LEGAL FRAMEWORK ON CYBERCRIME, In-text: (Chatham House, 2017), Your Bibliography: Chatham House. (2017). Building a Stronger International Legal Framework on Cybercrime. [online] Available at: https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime [Accessed 10 Sep. 2017].
- EUR-LEX - 32013L0040 - EN - EUR-LEX, In-text: (Eur-lex.europa.eu, 2017), Your Bibliography: Eur-lex.europa.eu. (2017). EUR-Lex - 32013L0040 - EN - EUR-Lex. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1440771959763&uri=CELEX:32013L0040 [Accessed 10 Sep. 2017].
- CYBERSECURITY, In-text: (Digital Single Market, 2017), Your Bibliography: Digital Single Market. (2017). Cybersecurity. [online] Available at: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity [Accessed 10 Sep. 2017].
- ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Accessed 10 Sep. 2017].
- ANON, In-text: (Anon, 2017), Your Bibliography: Anon, (2017). [online] Available at: http://russiancouncil.ru/papers/RIAC-EWI-Russia-US-Cybersecurity-Policybrief11-en.pdf [Accessed 10 Sep. 2017].
- CHINA PUBLISHES FIRST NATIONAL CYBERSECURITY STRATEGY, In-text: (Usito.org, 2017), Your Bibliography: Usito.org. (2017). China Publishes First National Cybersecurity Strategy. [online] Available at: http://www.usito.org/news/china-publishes-first-national-

cybersecurity-strategy [Accessed 10 Sep. 2017].

FURTHER READING

- MCQUADE, S. C., Understanding and managing cybercrime, In-text: (McQuade, 2006), Your Bibliography: McQuade, S. (2006). Understanding and managing cybercrime. Boston: Pearson/Allyn and Bacon.
- BRENNER, S. W. AND CLARKE, L. L., Combatting cybercrime through distributed security, In-text: (Brenner and Clarke, 2009), Your Bibliography: Brenner, S. and Clarke, L. (2009). Combatting cybercrime through distributed security. International Journal of Intercultural Information Management, 1(3), p.259.
- CALDERONI, F., A Definition that Could not Work: the EU Framework Decision on the Fight against Organised Crime, In-text: (Calderoni, 2008), Your Bibliography: Calderoni, F. (2008). A Definition that Could not Work: the EU Framework Decision on the Fight against Organised Crime. European Journal of Crime, Criminal Law and Criminal Justice, 16(3), pp.265-282.
- CHAIKIN, D., Network investigations of cyber attacks: the limits of digital evidence, In-text: (Chaikin, 2007), Your Bibliography: Chaikin, D. (2007). Network investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change, 46(4-5), pp.239-256.
- LIST, F. AND EUROPE, C., Full list, In-text: (list and Europe, 2017), Your Bibliography: list, F. and Europe, C. (2017). Full list. [online] Treaty Office. Available at: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. 9. [Accessed 11 Sep. 2017].
- LIST, F. AND EUROPE, C., Full list, In-text: (list and Europe, 2017), Your Bibliography: list, F. and Europe, C. (2017). Full list. [online] Treaty Office. Available at: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. 10. [Accessed 11 Sep. 2017].
- POUNDER, C., The Council of Europe Cyber-Crime Convention, In-text: (Pounder, 2001), Your Bibliography: Pounder, C. (2001). The Council of Europe Cyber-Crime Convention. Computers & Security, 20(5), pp.380-383.
- CYBERCRIME LAWS NEED OVERHAUL, In-text: (Cybercrime laws need overhaul, 2001), Your Bibliography: Cybercrime laws need overhaul. (2001). Network Security, 2001(1), p.3.
- EUR-LEX - 32005F0222 - EN - EUR-LEX, In-text: (Eur-lex.europa.eu, 2017), Your Bibliography: Eur-lex.europa.eu. (2017). EUR-Lex - 32005F0222 - EN - EUR-Lex. [online] Available at: http://eur-

lex.europa.eu/legal-content/EN/ALL/?uri=celex:32005F0222 [Accessed 11 Sep. 2017].
- EUR-LEX - 32001H0703(01) - EN - EUR-LEX, In-text: (Eur-lex.europa.eu, 2017), Your Bibliography: Eur-lex.europa.eu. (2017). EUR-Lex - 32001H0703(01) - EN - EUR-Lex. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001H0703(01) [Accessed 11 Sep. 2017].
- FLANAGAN, A., The law and computer crime: Reading the Script of Reform, In-text: (Flanagan, 2005), Your Bibliography: Flanagan, A. (2005). The law and computer crime: Reading the Script of Reform. International Journal of Law and Information Technology, 13(1), pp.98-117.
- GERCKE, M., Europe's legal approaches to cybercrime, In-text: (Gercke, 2009), Your Bibliography: Gercke, M. (2009). Europe's legal approaches to cybercrime. ERA Forum, 10(3), pp.409-420.
- GERCKE, M., National, Regional and International Legal Approaches in the Fight Against Cybercrime, In-text: (Gercke, 2008), Your Bibliography: Gercke, M. (2008). National, Regional and International Legal Approaches in the Fight Against Cybercrime. Computer Law Review International, 9(1).
- BUONO, L., Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches, In-text: (Buono, 2016), Your Bibliography: Buono, L. (2016). Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. ERA Forum, 17(3), pp.343-353.
- GORDON, S. AND FORD, R., On the definition and classification of cybercrime, In-text: (Gordon and Ford, 2006), Your Bibliography: Gordon, S. and Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), pp.13-20.
- CLOUGH, J., The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World, In-text: (Clough, 2012), Your Bibliography: Clough, J. (2012). The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World. Criminal Law Forum, 23(4), pp.363-391.
- DALLA GUARDA, N., Governing the ungovernable: international relations, transnational cybercrime law, and the post-Westphalian regulatory state, In-text: (Dalla Guarda, 2015), Your Bibliography: Dalla Guarda, N. (2015). Governing the ungovernable: international relations, transnational cybercrime law, and the post-Westphalian regulatory state. Transnational Legal Theory, 6(1), pp.211-249.
- KIERKEGAARD, S., Cybercrime convention: narrowing the cultural and privacy gap?, In-text: (Kierkegaard, 2007), Your Bibliography: Kierkegaard, S. (2007). Cybercrime convention: narrowing the cultural and privacy gap?. International Journal of Intercultural Information

Management, 1(1), p.17.
- SCHWERHA IV, J. J., Cybercrime: Legal Standards Governing the Collection of Digital Evidence, In-text: (Schwerha IV, 2004), Your Bibliography: Schwerha IV, J. (2004). Cybercrime: Legal Standards Governing the Collection of Digital Evidence. Information Systems Frontiers, 6(2), pp.133-151.
- SMITH, R., GRABOSKY, P. AND URBAS, G., Cyber Criminals on Trial, In-text: (Smith, Grabosky and Urbas, 2004), Your Bibliography: Smith, R., Grabosky, P. and Urbas, G. (2004). Cyber Criminals on Trial. Criminal Justice Matters, 58(1), pp.22-23.