

**OASIS INTERNATIONAL SCHOOL MODEL UNITED NATIONS**

General Assembly

 President: Hussein Fakharany

Vice-president: Malak Mounir

Guiding package

Topic (1): Measures to limit the use of the internet for terrorist purposes

10th Annual **OISMUN** conference

**Table of Contents**

I-Abstract……………………………………...page 3

II-Introduction………………….……………...page 4

III-Definition of key terms………..…………..page 5

IV-Background Information…….…………....page 6

V-Major countries/organizations involved….page 7

VI-UN Involvement…………..………….….page 11

VII-Possible Solutions……………………..page 13

VIII-Guiding Questions…………………….page 14

IX-Useful Links…………………………..…..page 15

X-Bibliography……………………………….page 17

1. **Abstract:**

 In the last couple of years, the world has encountered crucial and catastrophic terrorist attacks. Nevertheless, the incursions are not only in the form of the frequent bombing attacks, but cyberterrorist attacks as well as governments as well as citizens have witnessed interventions in their systems . Cyberterrorism is: “computer-based attacks aimed at disabling vital computer systems so as to intimidate, coerce, or harm a government or section of the population.[[1]](#footnote-0) In the furtherance of obtaining “Global stability through international cooperation, empowerments and innovation”,a resilient and stable cyberspace[[2]](#footnote-1) must be established among citizens of the world as well as governments .

 Cyberterrorism includes all illegal practicing of internet; such as revealing business/personal data, practicing hacktivism[[3]](#footnote-2), the publishment of false data, theft, etc.. Due to the increase of cyber terrorist attacks in the previous years, the attention of governments and several organizations has been drawn to that. Hence, after realizing that global stability will be at risk, efforts have been intensified in order to deal with that quandary. According to the ITU [[4]](#footnote-3), “cybersecurity” is a “set of security tools, policies, concepts, drivers, risk management methods, actions, education, awareness, good practices, insurances and technologies to protect users and organization assets in cyberspace”.[[5]](#footnote-4)

**II. Introduction**

 Our era has witnessed unbelievable scientific and technical innovations, inventions and life changing discoveries; all aiming to make the human daily life more stable, trouble-free as well as establish an innovative environment; one that can help the citizens live a normal healthy life therefore produce and help the community. Hence, the idea of a safe environment also applies on the innovation of Internet. The internet has been misused in different pivotal ways.

 The cyberspace has been a tool to terrorize people/governments, blackmail, and hack them. More specifically terrorists use the informations they lacked or fear of others to therefore obtain what they want (money, information against governments, and being in control of crucial decisions) . The proliferation of cybercrime is due to various ways such as the threats to governments making countries get involved in conflicts, the theft of millions of dollars using viruses, the threat of exposing as well as leaking any sort of personal dangerous information has been more clear. Our world has been more aware of the problem and is working on it, and the efforts continue. The subject of matter has drawn the attention of world leaders, organizations as well as the United Nations when Ban Ki-moon (UN current Secretary General) has commented on the topic stating that “The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.”

**III.** **Key terms**

**1- *Cyberterrorism:*** *“*computer-based attacks aimed at disabling vital computer systems so as to intimidate, coerce, or harm a government or section of the population.”

**2- *Cyberspace: “***the realm of electronic communication”

**3-*Hacktivism: “***the practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as a means of achieving political or social goals”

**4-*Terrorism:*** “The unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims” is the official definition of terrorism given by the English Oxford official dictionary[[6]](#footnote-5).

**5-*Cybersecurity: “***measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”[[7]](#footnote-6)

***6-Internet Governance:*** “Internet Governance can be defined as the evolving policies and mechanisms under which the Internet community’s many stakeholders make decisions about the development and use of the Internet.”[[8]](#footnote-7)

**7-*Telecommunication:*** “Communication over a distance by cable, telegraph, telephone, or broadcasting.”[[9]](#footnote-8)

**IV. Background information:**

 In our modern days, the definition of global stability and safety has been updated as it does also includes a safe cyberspace. Internet and modern technology have been easily accessible for users in the past few years. Almost half of the world’s population with 3.2 billion is connected to the internet[[10]](#footnote-9). Unfortunately we cannot limit the proliferation of information and communication technologies (ICTs). In fact the opportunity for real-time borderless exchange is growing. Hence, hackers and cyber terrorists are more likely to commit crimes frequently. Taking the example of Flame aka Skywiper and Flamer one of the major cyberattacks in history. Flame is a virus discovered in 2012 that spread among the Middle Eastern countries running through Microsoft Windows. “Used by hackers for espionage purposes, it infected other systems over a local network (LAN) or USB stick including over 1,000 machines from private individuals, educational institutions, and government organizations.”[[11]](#footnote-10) Other than the flame, “Iran was subjected to cyber attacks on June 2010 when its nuclear facility in Natanz was infected by Stuxnet, a cyber worm that was believed to be a combined effort of Israel and the United States, though no one claimed responsibility for its inception.” [[12]](#footnote-11) When Stuxnet hit Iran it damaged and caused the destruction of Tehran’s 1000 nuclear centrifuges. According to Norton study in 2011, there are one million cybercrime victims every day. Cyberattacks as a matter of privacy breach, targets citizens, businesses and governments. Thus it is considered as a global threat. MyDoom is a virus first discovered in 2004, “and it became **the fastest-spreading email worm ever**, exceeding all previous records. The virus’s origins are believed to be in Russia, but its author was never discovered.” [[13]](#footnote-12)Mydoom is still ranked as the most expensive virus in the world which damage costs 38.5 billion dollars.

**V. Major countries involved:**

***The United States of America:*** is involved in several ways. Since cyberattacks have been known in the world (among governments and citizens), the USA has been fighting and preparing against those attacks. According to WEFORUM the USA is the country most prepared for cyber attacks around the world. They are keeping up and are updated with the problem, and have the most developed cybersecure systems around the world. Donald Trump, the U.S president, promised in his pre-elections speech to continue the efforts already started as well as make cybersecurity “an immediate and top priority for my administration” . Nevertheless, the USA is also involved as a source of cybercrime. It has been identified[[14]](#footnote-13) that a major number of cyberattacks are originated from the USA; whether in its territories or out. The USA stated in The EastWest Institute summit that they blame Russia and China for all sorts of cyberattacks.

***The Republic of Estonia:*** In 2007, a virtually fatal cyberattack hit Estonia. BBC news identified the issue as “How a cyberattack transformed Estonia”. Estonia has witnessed the first well-known cyberattack to hit an entire country. Starting then, Estonia has been a victim of crucial cyberattacks that can last for a couple of weeks. These cyberattacks had an impact on the government as well as citizens. Cash machines and online banking services were hacked as well as ministries, Estonian parliament, newspapers and broadcasters. Since then, Estonia took part in several organizations aiming to solve that issue. The April 27th 2007 attack was in the middle of Estonia’s disagreement with Russia concerning the relocation of the Bronze Soldier of Tallinn. Therefore Russia was blamed for those cyberattacks, but the country denied the responsibility.

***The Russian Federation:*** has been blamed by the US, Estonia and several other countries for most of the cyberattacks they’ve suffered from since 2007. This accusation has also been taken into consideration when the Russian Federation hasn't been listed among the top 20 cyber secured countries[[15]](#footnote-14). Followingly, some countries have stated that Russia does not need cybersecurity bearing in mind that they are the source of cybercrime.

**Major Organizations Involved:**

***Global Cyber Security Center (GCSEC):*** is a non-profit Italian organization. The organization’s purpose is to advance and innovate cybersecurity in Italy, the region and the entire world. The Center is funded by Poste Italiane[[16]](#footnote-15) and based in Rome, the organization relies on “a strong collaboration with Italian and International government institutions, private bodies, research institutions and international bodies.

The mission of the center is to develop and disseminate knowledge and awareness on Cyber Security, creating the conditions for improving capabilities, skills, cooperation and communication between the different stakeholders involved in the use and protection of internet.” [[17]](#footnote-16)

***The Center for Internet Security:*** is a non profit organization located in New York and founded in 2000, aiming to “enhance the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration.”The organization has 180 members coming from 17 different nationalities all working for the same purpose and mission. The center for internet security has four different sections: the Central Intelligence Center, the Multi-State Information Sharing and Analysis Center, Security Benchmarks, and the Trusted Purchasing Alliance. Using those four divisions, and relying on its collaboration, the organization works extremely hard to establish a safe virtual environment.

***The International Information Systems Security Certification Consortium:*** is certified as the world’s leading cybersecurity organization, headquartered in the USA, nevertheless has diverse offices in several countries around the world. The (ISC)² has over 125 000 members of cyber, and IT professionals. The organization has been certified as the best, because of its awareness that the key to solve this issue is to work day by day consistently.

***The SANS Institute:*** “was established in 1989 as a cooperative research and education organization.”[[18]](#footnote-17) It works on a different aspect of the quandary, as this institute does not work on solving the problem itself; but rather maintaining a sustainable solution that’ll protect the cyberspace forever. The technique used by the SANS institute is to make use of young minds and sustainably solve the problem from the roots using courses for young adults to raise their awareness concerning the problem and teaching them how to make the cyberspace more secure.

**VI. UN involvement:**

Concerning that complication, all the UN’s efforts were dedicated towards the creation of Organizations/offices as well as organizing special events aiming to find solutions to the chaotic problem.

* ***The United Nations Office on Drugs and Crime (UNODC):*** was not based or founded for the purpose of cybersecurity despite so, it is an office responsible for different sorts of crimes (including cyber crime). The UNODC, has presented a full report stating the problem’s details, causes, laws against it all around the world, as well as ways to prevent it. Taking the example of a report conducted 2013 with the title “Comprehensive study on cybercrime” [[19]](#footnote-18) and another report in My 2011 with the title: “Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects” [[20]](#footnote-19)
* ***Counter terrorism implementation task force:*** is a working group responsible of establishing and implementing decisions by the UN concerning terrorism. The group has presented a report countering the use of internet for terrorist purposes. [[21]](#footnote-20) The counter terrorism implementation task force is responsible of ensuring that each decision made by the UN concerning terrorism is being applied efficiently as decided by the UN.

**Extract from the UNODC report: [[22]](#footnote-21)**

“28. A cyberattack generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware flooding or other means of unauthorized or malicious hacks

“29. While terrorists have developed many ways to use the Internet in furtherance of illicit purposes, their use of the Internet also provides opportunities for the gathering of intelligence and other activities to prevent and counter acts of terrorism, as well as for the gathering of evidence for the prosecution of such acts. A significant amount of knowledge about the functioning, activities and sometimes the targets of terrorist organizations is derived from website, chat room and other Internet communications. Access.”

**VII. Possible Solutions:**

1. Enforcing severe security and monitoring programs on different regions especially on the ones who may be responsible of such act. .
2. Endorsing strict international laws to apply them against hackers and cyberterrorists.
3. Encouraging internet users to use anti-viruses and internet security programs in order to protect themselves in case of cyber attacks.
4. Founding a committee which members will be experts in the field, who will keep track of the problem and update governments as well as find solutions. The committee will also work with the SANS institute therefore be the first to gather the statistics of the courses and be able to predict and prepare for future attacks and development of the cyberspace.
5. Raise awareness among citizens of the world, to prevent any hacking and breach of privacy on their personal devices through social media, radio, journals..etc

**VIII. Guiding Questions:**

1-What are the main problems that make the process of sustainably solving cybercrime hard?

2-What have the organisations done until now to solve the issue and have those efforts improved the situations?

3-Has your country done any efforts concerning the problem? If Yes, what are those efforts?

4-Is your country lacking cybersecurity? Is your country a victim of cybercrime? Is your country considered as an origin of cybercrime and hacktivism?

5-What are the solutions that could solve the problem from its roots?

6-Are there national laws in your country against cyberterrorists?

**IX. Useful links:**

* NETMUNDIAL, available on: <http://www.globalmediapolicy.net/sites/default/files/Cybersecurity%20thoughts%20and%20issues%20from%20a%20political%20perspective.pdf> , consulted 17/07/2017
* UNITED NATIONS DEPARTEMENT OF ECONEMENT AND SOCIAL AFFAIRS, available on: <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html> , consulted 17/07/2017
* MACASKILL, Ewen, available on: <https://www.theguardian.com/technology/2010/may/05/terrorism-uksecurity>, consulted 15/07/2017
* WONG, Julie-Carrie, available on: <https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs>, consulted 15/07/2017
* GROSS, Grant, available on: <http://www.computerworld.com/article/2492864/cybercrime-hacking/un--more-international-cooperation-needed-to-fight-cyberterrorism.html> , consulted 16/07/2017
* COUNTER TERRORISM IMPLEMENTATION TASK FORCE, available on: <http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf>, consulted 17/07/2017

**X. Bibliography:**

* Dictionary.com Unabridged. Available on <http://www.dictionary.com/browse/cyberterrorism>, Consulted 17/07/2017
* English Oxford living dictionary , available on <https://en.oxforddictionaries.com/definition/terrorism> consulted 17/07/2017
* SANTIAGO, Joe, available on <https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/> consulted 18/07/2017
* GLOBAL CYBER-SECURITY CENTER (GCSEC), available on <https://www.gcsec.org/> consulted 18/07/2017
* THE SANS INSTITUTE, available on <https://www.sans.org/about/> consulted 18/07/2017
* UNITED NATIONS OFFICE ON DRUGS AND CRIME,available on <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> consulted 18/07/2017
* UNITED OFFICE ON DRUGS AND CRIME, Available on <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>, consulted 03/08/2017
* BAIG, Anas, available on: <https://securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx>, consulted 16/07/2017
* JOSEF, Smith, available on <http://list25.com/25-biggest-cyber-attacks-in-history/m>, consulted 03/08/2017
* The number resource organization, available on <https://www.nro.net/nro-and-internet-governance/> , consulted 17/07/2017
1. Dictionary.com, available on <http://www.dictionary.com/browse/cyberterrorism>,

consulted 17/07/2017 [↑](#footnote-ref-0)
2. Dictionary.com, available on <http://www.dictionary.com/browse/cyberspace> consulted July 17, 2017 [↑](#footnote-ref-1)
3. Dictionary.com available on <http://www.dictionary.com/browse/hacktivism> consulted July 17, 2017 [↑](#footnote-ref-2)
4. the International Telecommunication Union [↑](#footnote-ref-3)
5. Guadalajara Resolution 181, 2.010 [↑](#footnote-ref-4)
6. English Oxford living dictionary , available on <https://en.oxforddictionaries.com/definition/terrorism> consulted 17/07/2017 [↑](#footnote-ref-5)
7. Merriam Webster, available on <https://www.merriam-webster.com/dictionary/cybersecurity> , consulted 17/07/2017 [↑](#footnote-ref-6)
8. The number resource organization, available on <https://www.nro.net/nro-and-internet-governance/> , consulted 17/07/2017 [↑](#footnote-ref-7)
9. English Oxford living dictionary , available on <https://en.oxforddictionaries.com/definition/telecommunication> , consulted 17/07/2017 [↑](#footnote-ref-8)
10. Estimated in 2015 by the International Telecommunication Union [↑](#footnote-ref-9)
11. JOSEF, Smith, available on <http://list25.com/25-biggest-cyber-attacks-in-history/m> consulted 03/08/2017 [↑](#footnote-ref-10)
12. Ibid [↑](#footnote-ref-11)
13. Heimdal security, available on <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/> consulted `17/07/2017 [↑](#footnote-ref-12)
14. BAIG, Anas, available on: <https://securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx>, consulted 16/07/2017 [↑](#footnote-ref-13)
15. SANTIAGO, Joe, available on <https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/>, consulted 18/07/2017 [↑](#footnote-ref-14)
16. Postal service company [↑](#footnote-ref-15)
17. GCSEC, available on <https://www.gcsec.org/> consulted 18/07/2017 [↑](#footnote-ref-16)
18. The SANS institute, available on <https://www.sans.org/about/> consulted 18/07/2017 [↑](#footnote-ref-17)
19. UNITED OFFICE ON DRUGS AND CRIME, Available on <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> consulted 03/08/2017 [↑](#footnote-ref-18)
20. UNITED NATIONS, Available on <http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf> consulted 18/07/2017 [↑](#footnote-ref-19)
21. Ibid [↑](#footnote-ref-20)
22. The use of the Internet for terrorist purposes In collaboration with the United Nations Counter-Terrorism Implementation Task Force, available <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> consulted July 18 2017 [↑](#footnote-ref-21)