MSMUN 2019

DISEC

Disarmament and International Security Committee

Official language: English

Chair:

María José Jaramillo

María Camila Giraldo

Topic:

Cyber Terrorism and arm traffic through the Deep Web.

Table of Contents

1. Welcoming Letter:

Distinguished delegates,

We are Maria Camila Giraldo, and María José Jaramillo; and this year we have the incredible opportunity and honor to preside over the United Nations Disarmament and International Security Committee of MSMUN Internal Model 2019.

Through our experience in Models of the United Nations, we have discovered that these are very enriching spaces, referring not only to academic skills, but also to social and personal skills; and because of this, we hope that you prepare yourselves very well, that you research and learn a lot, give your best, participate, have a great and positive attitude, and get a fascinating experience in which you challenge yourselves and get out of your comfort zones, testing your skills and acquiring or discovering new ones.

We want you not only to learn from a debate, but from other delegates and their points of view, and in order to achieve this, it is necessary to listen carefully, be respectful, work as a team, and be open-minded, so that you can get to an agreement that seeks for what is needed in the committee. Also, we encourage you to try to look for and offer viable solutions to solve global issues (in this case cyber terrorism and arm traffic through the Deep Web), with the hope of making a better future.

Finally, we hope that you enjoy the committee, and that you have the chance to grow as delegates, but mainly, as citizens of the world and human beings.

Welcome to the United Nations´ Disarmament and International Security Committee. Please remember that we are here to help you with anything you need. Don't hesitate in contacting us if you have any question or doubt.

Very truly yours,

María José Jaramillo and **Maria Camila Giraldo**

Marymount School Medellín

mariajojara15@gmail.com mariacamigq@gmail.com

2. United Nations Disarmament and International Security Committee:

2.1. Commission's history and objective:

The United Nations Disarmament Commission was created in 1952 by the United Nations General Assembly Resolution 502 (VI). It was conceived based on article 11 of the United Nations Charter, in which the General Assembly should consider the principles that lead to the maintenance of international peace and security, including disarmament and the regulation of armaments (United Nations, 2019). This committee "deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime" (United Nations, 2019).

This commission adopted the topic entitled "Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy" in the very first General Assembly. This commission is considered as the First Committee of the General Assembly, it meets once every year, and has the purpose of creating cooperation in the maintenance of peace and security around the globe, taking into account the regulation of armaments. Additionally, it works in collaboration with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament.

3. Topic: Cyber terrorism and arm traffic through the Dark Web:

3.1. Theoretical framework:

Nowadays people with extremist ideas and intentions, have opted for tools such as the internet, which provides unlimited access to information and sources, in order to carry out operations and commit illegal acts, but the Internet is a very wide platform that has multiple uses, and is divided into various parts, and because of this, it is important to understand its portions and engines and the differences between them, and the types of crimes and actions that are carried out. Also, it is essential to take into account that some parts of the internet, mostly the Dark Web, which is mainly used for illegal activities, have been used by multiple criminal groups and organizations to traffic weapons in a more efficient and easy way.

Cyberspace: "Refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication." (Techopedia, 2019).

Cyber terrorism: "According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents." (Ferguson, Rosencrance, and Rouse, 2019).

Cyber Warfare: "Cyber Warfare is computer- or network-based conflict involving politically motivated attacks by a nation-state on another nation-state." (Ferguson, Rosencrance, and Rouse, 2019).

Cybercrime: “The USA department of justice defines computer crime as “any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution” (Tafazzoli, 2018).

Surface Web: The normal web which is visible for all users using internet. The websites in the surface web is indexed by search engines. Google is the great example of search engine. The user can open websites and gain information (Hackers League, 2018).

Deep Web: “Sometimes called the invisible Web, is the large part of the Internet that is inaccessible to conventional search engines.” (Rouse, 2016).

Dark Web: “Also referred to as the dark net, is an encrypted portion of the internet that is not indexed by search engines. The dark web is a subsection of the deep web” that is mainly used for illegal activities. (Rouse, 2017).

Cyber Security: “The techniques of protecting computers, networks, programs and data from unauthorized access or attacks.” (Economic Times, 2019)

TOR: The Onion Router. Allows individuals to access the Darknet. “It can make layers of many IPs and the user surf the internet anonymously. Many dark web websites are banned by Tor but the dark web is totally not cleared.” (Hackers League, 2018).

Arm Trafficking: Trafficking firearms involves the manufacture and illegal distribution of firearms, their components and ammunition (Salcedo and Santos, 2017).

Darknet Market: Dark web sites with goods for sale (Frankenfield, 2018).

3.2. History of the topic.

The term “Cyber terrorism”, which refers to “premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against noncombatant targets” (Pollitt, 2019), was first conceived in the 1980’s by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. This term was initially represented by the first cyber-attack recorded in history in 1988 in the United States, called the “Morris Worm”, in which Robert Tappan Morris created a program that traveled through computers and sent signals back to a control server, and this ended up clogging up large sections of the Internet (Shackelford, 2018).

After this incident, there have been lots of other types of cyber-attacks in different countries throughout history:

As we can see, throughout the years, Cyber terrorism has developed and evolved, and has been applied by multiple groups and persons that commit terrorist actions, due to the fact that it is cheaper/free, anonymous, unlimited, and easy to carry out; with the motivation that consists of blackmail, destruction of information and data, exploitation and revenge, attack on computer systems, and access to services, data, and systems (Vilić, 2017).

Terrorists have been active on multiple online platforms since the late 1990's (Weimann, 2004), and they not only use the Dark net, which has been throughout the years the cradle of criminal activity and black markets in the web, in order to hide and commit their crimes without being identified, but also to traffic weapons and drugs, spread news and propaganda, communicate, recruit new followers, and plot future attacks.

Since 2012, the Dark net (which was first coined in the 1970's) has been used by terrorist groups with the purpose of transferring and raising funds illegally (using virtual currencies such as Bit coin), and acquiring and purchasing explosives and weapons, taking into account that it is an enabler for the circulation of illegal weapons, considering that the transaction and acquisition of the weapons is completely anonymized, and this platform increases the availability of more recent, better performing, and cheaper arms (Paoli, Aldridge, Ryan and Warnes, 2017). Throughout the years, there have been numerous commerce sites used for traffic of illicit products including arms, drugs, malignant computer programs, and stolen data such as AlphaBay and Hansa (which were closed in 2017 due to an investigation that was carried out by the police of the United States (FBI) and Europe (Europol)) (Baraniuk, 2017). The majority of the content and sites of the Deep Web and Dark net are illegal, and due to this, they cannot be accessed through common search engines and because of this, it is necessary to use other protocols and tools such as TOR, which is the most known. Tor was created in 2002 with the purpose of hiding the user's identities. Instead of being connected directly with the server in which products are sold, there are multiple jumps of anonymity to prevent the user's activities and itself from being tracked (Jaramillo, 2018).

Terrorist groups such as Anonymous, ISIS and other jihadist groups, have turned to the Dark net to communicate their information and messages, and to protect the identities of their supporters (Weimann, 2004).

"OpParis" is one of the campaigns/strategies that have been used to take down websites that are associated with terrorist groups. Also, the Defense Advanced Research Projects Agency thinks that MEMEX is an efficient solution, which is a software that allows cataloguing Deep Web sites, monitoring human trafficking on the Deep Web, being able to apply this principle to almost any illicit Deep Web activity (Vilić, 2017).

Also, the American National Infrastructure Protection Center devotes its work to combat cybercrime and created the National Infrastructure Protection Plan in 2013. Yet, Cyber terrorism has a partner that makes this attacks and cases much easier, being the Deep and Dark Web, which facilitates the elaboration of illegal acts.

The Internet is divided into three main stages, the *Surface Web, Deep Web*, and *Dark Web*, and the last two are the ones that contain 96% of it, the remaining 4% corresponding to social media (Relancio, 2017).

3.3. Situation today:

Cyber terrorism in the 21st century is one of the greatest threats to global security and information as it can cause massive loss of life, worldwide economic and political chaos, environmental damage, and loss of security and information; and eventually, it will become more frequent and popular due to the easiness of the management of the Web. The Internet has become a tool that throughout the years has enabled people from different parts of the world to meet, communicate, express, exchange and share ideas and opinions, and provide access to different types of knowledge, information and content that may be useful for everyday activities and duties; but it has also been used and implemented by extremist people and organizations of various types to carry out operations and distribute and communicate propaganda, ideas and concepts (Weimann, 2004).

As of today, terrorists opt for methods that facilitate their operations, and frequently they've concurred to methods that involve technology, due to the fact that they are cheaper than traditional methods, are anonymous, don't have physical barriers and borders, the number of targets is huge, don't have regulations, have a fast flow, have inexpensive maintenance and development and can be conducted remotely, avoiding many types of risks (Weimann, 2004).

The Dark Web is one of the tools that have enabled the circulation of illegal weapons that come from the black market, and it contains multiple avenues for criminals to bypass controls and traffic merchandise, especially weapons across international borders. Also, it hosts multiple online black markets that make easier the sale and traffic of weapons, explosives, firearms, and banned digital materials that are better performing and more recent for relatively low prices, and with the advantage of being completely anonymous.

(Vilić, 2017). The procedure needed to be taken is really simple; “The markets are accessible via the Tor network or other browsers that protect the user’s identity and location. Transactions take place via Bit coin using dark wallets to protect the seller and the buyer. The payment is held in escrow by the site operator to discourage scammers. The only exposed link in the chain is the actual shipping of the goods through the postal system. To reduce the risk, dark net market customers may rent a post box or use an address they don’t own but can access” (Frankenfield, 2018).

3.4. Nation's pronounces towards the topic:

The United States appears to be the most common source country for arms that are for sale on the dark web, and approximately 60% of the firearms listing are associated with products that originate from the United States; but it is important to take into account that Europe contains the largest market for arms trade on the dark web, generating revenues that are around five times higher than the United States. (Paoli, Aldridge, Ryan and Warnes, 2017).
Also, statistics that refer to the worldwide distribution of dark net firearm vendors by country in 2017 show some countries such as: the United States, with 59.29%, Denmark, with 12.98%, Germany, with 5.31%, the United Kingdom, with 1.47%, and Canada, with 0.59%. (Statista, 2017).

Multiple countries have carried out strategies in order to combat cyber terrorism and have protection against these attacks such as STIC, which refers to the set of security measures to protect the information stored, transmitted and processed by telecommunication and

information systems, in order to guarantee and ensure the integrity, confidentiality, and availability of the information and the system itself. (Fernández, 2019).

Taking into account the great impact that cyber terrorism has had lately, various countries around the globe have worked to have more protection, and some of the countries that are best prepared for cyber-attacks are the United States of America, Canada, Australia, Malaysia, Oman, New Zealand, Norway, Brazil, Estonia, Germany, India, Japan, the Republic of Korea, United Kingdom, Austria, Hungary, Israel, Netherlands, Singapore, and Latvia. (Santiago, 2015).

Also, it's important to highlight that some countries have more developed knowledge and practices of cyber terrorism, and some of them are China, Russia, United States, Turkey, Brazil, South Korea, India, Spain, Thailand, and Japan. (Chandran, 2016).

Finally, it is essential to take into account that there are various countries that are very vulnerable to cyber-attacks due to the lack of security, practices, and measures taken in order to fight this phenomenon, and some of them are Belgium, Dominican Republic, Hong Kong, Samoa, China, Afghanistan, Tajikistan, and South Africa. (Goud,2019).

4. QUARMAS:

1. Does your country have organizations that fight Cyber terrorism?
2. Do cyber-attacks originate in your country?
3. What have been the most serious and known cyber-attacks in your country's history, and who were the main actors?
4. What are the main types of cyber-attacks in your country?
5. Has your country used this 'methods' (entrances in the Deep Web, or Cyber-attacks) with others countries?
6. Does your country have protection against Cyber terrorism?
7. What measures has your country carried out to fight Cyber terrorism?
8. Are there any recognized groups or organizations that practice cyber terrorism in your country?
9. Do websites for arm trafficking originate in your country?
10. What types of weapons are trafficked in your country?
11. What are the main countries that have trafficking arrangements with your country?
12. What countries are the main arms suppliers of your country?
13. What web pages used for arm traffic are available in your country?
14. What measures do you consider can be implemented to stop and fight cyberterrorism and arm traffic in your country and eventually worldwide?

5. Bibliography:

United Nations. June 2019. *United Nations, main body, main organs, General Assembly.* Retrieved from https://www.un.org/en/ga/

United Nations. June 2019. *Charter of the United Nations.* Retrieved from https://www.un.org/en/charter-united-nations/

Techopedia. June 2019. *What is Cyberspace?*. Retrieved from https://www.techopedia.com/definition/2493/cyberspace

Rouse, M. May 2019. *What is cyber terrorism?.* Retrieved from https://searchsecurity.techtarget.com/definition/cyberterrorism

Rouse, M. May 2019. *What is cyber warfare?.* Retrieved from https://searchsecurity.techtarget.com/definition/cyberwarfare

Tafazzoli, T. May 2018. *Cybercrime Legislation.* Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime legislations.pdf

Hackers League. January 07, 2019. *What is Surface Web, Deep Web and Dark Web?.* Retrieved from https://medium.com/@hackersleague/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5

Rouse, M. July 2016. *What is deep Web?.* Retrieved from https://whatis.techtarget.com/definition/deep-Web

Rouse, M. July 2019. *What is the Dark Web and Top Security Concerns?*. Retrieved from https://whatis.techtarget.com/definition/dark-web

Economic Times. June 2019. *Definition of Cyber Security: What is Cyber Security ? Cyber Security Meaning.* Retrieved from https://economictimes.indiatimes.com/definition/cyber-security

Hackers League. January 07, 2019. *What is Surface Web, Deep Web and Dark Web?.* Retrieved from https://medium.com/@hackersleague/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5

Shackelford, S. November 05, 2018. *What the world's first cyber-attack taught us about cyber security.* Retrieved from https://www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges

Nato. 2019. *The history of cyber-attacks - a timeline*. Retrieved from https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

Weimann, G. 2019. *Going Darker?* Retrieved from https://www.wilsoncenter.org/sites/default/files/going_darker_challenge_of_dark_net_terrorism.pdf

Vilić, V. (2017). *Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyberspace.* Retrieved from https://www.researchgate.net/publication/324720749_DARK_WEB_CYBER_TERRORISM_AND_CYBER_WARFARE_DARK_SIDE_OF_THE_CYBERSPACE

Weimann, G. March 2004. *How modern terrorism uses the Internet*. Retrieved from https://books.google.com.co/books?hl=es&lr=&id=a_cugt6quTYC&oi=fnd&pg=PA2&dq=internet terrorism

Weimann, G. December 2004. *Cyber terrorism, How Real is the Threat?* Retrieved from https://www.usip.org/sites/default/files/sr119.pdf

Paoli, G. 2019. *International arms trade on the dark web*. Retrieved from https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html

World Economic Forum. 2019. *Top countries best prepared against cyber-attacks.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Top-countries-best-prepared-against-cyberattacks.aspx

Nagraj, A. July 14, 2016. *Revealed: 10 countries from where most cyber-attacks originate.* Retrieved from https://gulfbusiness.com/revealed-10-countries-from-where-most-cyber-attacks-originate/

Goud, N. March 22, 2017. *List of Countries which are most vulnerable to Cyber Attacks.* Retrieved from https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/

Salcedo, E. November 2017. *Introduction to firearms trafficking.* Retrieved from https://www.researchgate.net/publication/322340845_Introduction_to_Firearms_Trafficking

https://www.quora.com/What-is-the-difference-between-the-dark-web-and-the-deep-web

Frankenfield, J. February 14, 2018. *Darknet market definition.* Retrieved from https://www.investopedia.com/terms/d/darknet-market-cryptomarket.asp

Baraniuk, C. July 20, 2017. *Duro golpe contra los traficantes de armas y drogas en la internet oscura: FBI y Europol cierran los mercados AlphaBay y Hansa.* Retrieved from https://www.bbc.com/mundo/noticias-internacional-40674538

Jaramillo, M. June 10, 2018. *El mundo nauseabundo de la 'internet profunda'.* Retrieved from https://elpais.com/tecnologia/2018/05/29/actualidad/1527607959_693554.html

Paoli, G; Alridge, J; Ryan, N and Warnes, R. 2017. *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.* Retrieved from https://www.rand.org/pubs/research_reports/RR2091.html

Relancio, A. September 7, 2017. *Qué es Surface Web, Deep Web y Dark Web.* Retrieved from https://www.seas.es/blog/informatica/que-es-surface-web-deep-web-y-dark-web/

Routley, N. July 8, 2017. *The Dark Side of the Internet.* Retrieved from https://www.visualcapitalist.com/dark-web/

McCarthy, N. March 22, 2018. *Where guns are sold through the Darknet.* Retrieved from https://www.forbes.com/sites/niallmccarthy/2018/03/22/where-guns-are-sold-through-the-darknet-infographic/#4a0cd8f9647a

Fernández, F. 2019. *Protección de infraestructuras críticas frente al ciberterrorismo.* Retrieved from https://reunir.unir.net/bitstream/handle/123456789/3073/FranciscoJesus_Fernandez_Fernandez.pdf?sequence=1&isAllowed=y