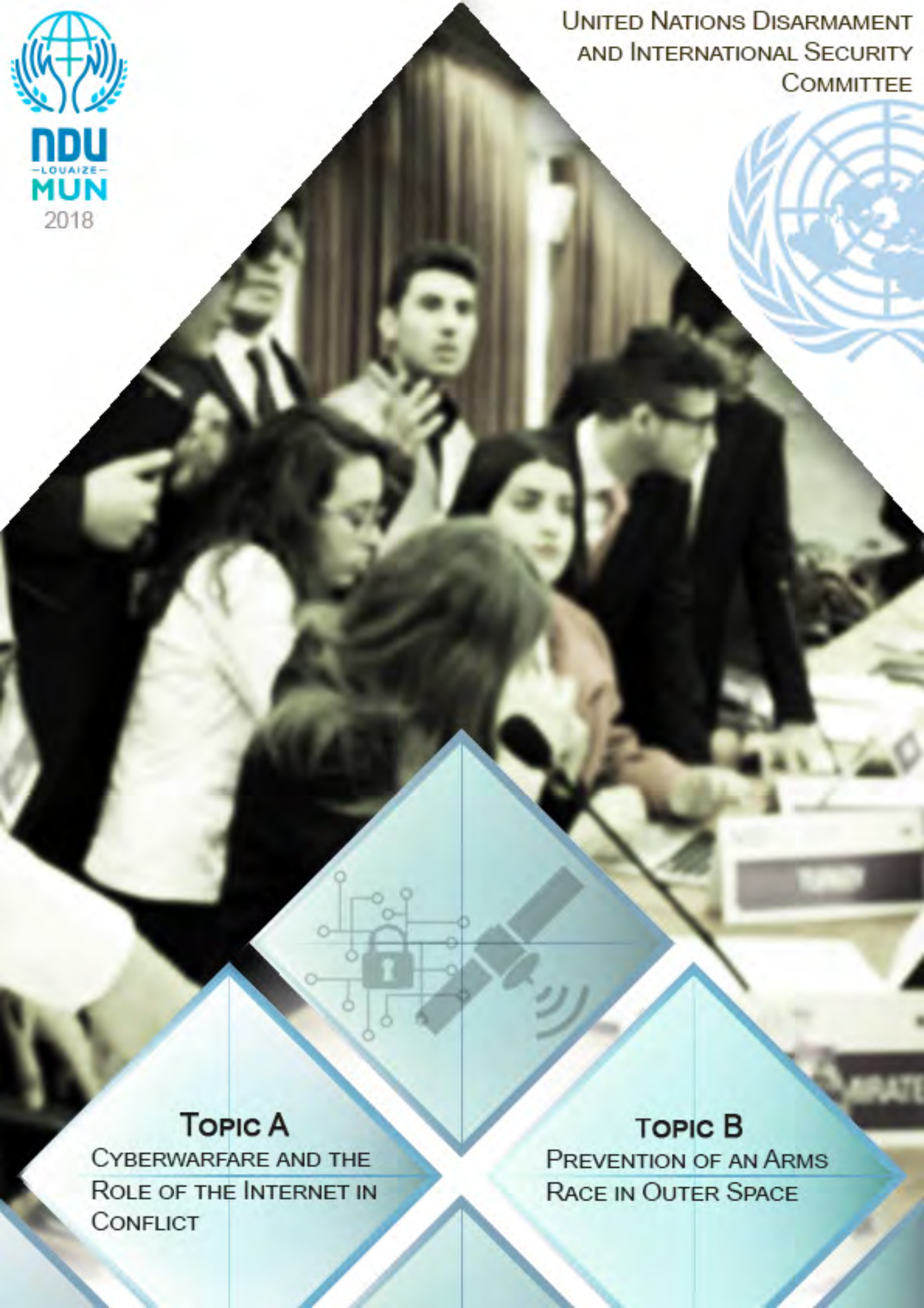
NDU
LOUAIZE
MUN
2018

United Nations Disarmament and International Security Committee



Topic A
Cyberwarfare and the Role of the Internet in Conflict

Topic B
Prevention of an Arms Race in Outer Space

Dear Esteemed Delegates,

"We strive to reach excellence, and we aim to achieve it."

On behalf of the Academic Training Committee, I welcome you all into our 2nd Annual Model United Nations Conference at NDU!

My dearest delegates, we live in a fallen world where the voice of reason is lost and the power of freedom is forgotten, where man is often seen to be poisoned by greed and blinded my misery and bloodshed, and where man can be the voice of change, but has failed to do so. But, you delegates, can be different. You have the power of change within you. So be courageous and stand up for what you believe in. Believe in yourself and believe in your country. But most importantly, believe that your voice will be heard.

In the conference, you will be representing a country that may not be your own. You will be representing the voice of a nation that you may not have heard of before. You will be the reason behind which a nation may stand or fall, and with that lies great responsibility. You will have to fight to make your voice heard, and I urge you delegates to keep fighting. Fight life the same way you will fight in that conference. For when you choose to create change, you will make your country proud, and you will make your school proud, because you chose to be THAT change.

I hope that, in return, you will leave the conference with more than just an award. You will leave the conference with everlasting memories, friendships that last a lifetime, and strong determination to handle life the same way you handled your conference.

Humbly Yours,
Stephanie Sleilati
Head of Academic Training

Dear Delegates,

The dais and I are excited to welcome you to the Disarmament and International Security Committee (DISEC) for the second NDUMUN conference.

I am your Chair for the upcoming days, my name is Perla Sawma, majoring in Computer and Communication Engineering. I would like to mention that I am very eager to be able to share with you these two fun constructive days of negotiations and debates.

Through NDUMUN, as well as the preparation leading up to it, the dais and I hope to ignite a passion for bridging differences in all of our delegates.

Both topics at hand are very interesting and negotiable, since countries all over the world have different opinions and stances regarding the issues at hand. The prevention of an arm race in outer space has become a part of the UN agenda this year since we cannot neglect the fact that with all the technology surrounding us we can easily turn outer space into a weapons stock. Also when it comes to cyberwarfare and how the internet plays an enormous role specifically in conflict zones as it might turn countries against each other's or even be the ignite of a revolution.

Every delegate is expected to be well researched with both the agendas and also to be aware of the stance the country he/she is representing.

In order to provide the best experience for all involved, make your voice heard throughout the weekend of discussions, whether it be through giving speeches in committee, passing notes to forge alliances, or by drafting and redrafting working papers.

If at any point our instructions and expectations are unclear, do not hesitate to reach out by email.

Looking forward to meet every single one of you!

Sincerely,
Perla Sawma
Chair of the Disarmament and International Security Committee

DISEC

Outline

— Disclaimer —

- *Notre Dame University & its Model United Nations program are diligent in promoting human rights & respecting international law.*
- *This guide does not represent the views of Notre Dame University, the NDU MUN program, or any of its members.*
- *All NDU MUN members reserve the right to the privacy & discretion pertaining their individual opinions on all issues.*
- *This guide remains neutral throughout & is not meant to sway public opinion on these sensitive & controversial issues.*
- *This guide features a panoply of references to back up the material being displayed*

— Disclaimer —

General Overview

A. Introducing the Committee:

The Disarmament and International Security Committee (DISEC) is the First Committee of the United Nations General Assembly (GA). Along with the other five General Assembly committees, this committee began with the founding of the United Nations in 1945, under Chapter IV of the United Nations (UN) Charter.

It includes all nations that are United Nations Member States, which is a total of 193 member states. The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament. It is the only Main Committee of the General Assembly entitled to verbatim records coverage.

B. Actions of the Committee:

The Disarmament and International Security Committee (DISEC) is given its powers by Chapter IV, Article 11, Sub-article 1 of the United Nations Charter, which states that the General Assembly "may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments, and may make recommendations with regard to such principles to the Members or to the Security Council or to both."

In fact, DISEC does not hold the power to pass treaties, laws, and policies. Yet, this committee can propose and recommend potential ones. Even though DISEC's jurisdictive authorities are limited to only stating out suggestions, it is still one of the most effective committees in the General Assembly. Its actions and recommendations are directed up to the Security Council, which possesses the power to turn those suggestions into action. The duty of this committee is to maintain international peace and security. So, as the name 'Disarmament' suggests, the committee aims to control and reduce the weaponry that is being owned, produced and traded all over the world. This leads to dealing with the illegal transport of small firearms, ensuring that nuclear weapons are not being used by any nation, and newly resolving the issue of cyber-attacks that are targeting the safety and well-being of various countries.

Topic A
Cyberwarfare and the Role of the Internet in Conflict

I. Definition of Topic:

The first workable prototype of the Internet came in the late 1960s with the creation of ARPANET (Advanced Research Projects Agency Network).The first message across ARPANET was sent on October 29th, 1969.The Internet is a global network of billions of computers and other electronic devices that can access almost any information and it is also the base of communication. [30]

Since its launch, the internet has been rapidly progressing. It became an important part of most governments' infrastructure. Governments rely on technology and internet in many aspects; to store classified information, perform tasks more accurately and efficiently, control military weapons, provide platforms that allow people to access information and to communicate within the government and with others. The increasing dependency on the internet results in an increased vulnerability to attacks.

The term "cyber warfare" refers to the use of internet as a mean of war by distorting or destroying classified information or computer programs involved in military operations [1]. Cyber-attacks present a major threat to all governments and organizations connected to the internet. Since nowadays the world is so dependent on cyberspace and social media accounts, a lot of countries are victims of different types of cyber-attacks. Starting with the Phishing Attacks where hackers send out thousands of emails, with an attachment or a link, so that they can have access to computer systems and all the information on them. As for Spyware, hackers introduce a software that tracks keystrokes to get passwords or electronically spy on networks to gain access to confidential information. Also, Hijacking Session or the Man in the Middle Attack, where the attacker steals the session ID that should stay private between the user and the remote web server, and he poses himself as the user which leads him to gaining access to gaining access to unauthorized data on the web server.[29]

These attacks can be sabotage attacks that aim to disrupt, destroy or distort information, or espionage attacks that are intended to spy on a certain country for example to access classified data[34]. Improving cyber-security is a logical solution to this issue at hand, however the cyber attackers, with their improved abilities, makes it difficult to achieve it.

Besides the role of the internet on the national and governmental level, the internet dominates the lifestyle of many people worldwide and enables them to express their opinion on different topics freely. The freedom of expression provided by different social media platforms can be used as a powerful tool by the society (e.g.: Pressuring the government to legislate a new law). Nevertheless, as much as the internet can be used to cause a positive change or to protest oppressed rights, it can also be a dangerous tool used for inciting conflicts.

II. Role of Committee in Current Topic:

The UN efforts to regulate cyberspace have been rudimentary at best. It was first adopted to the General Assembly‘s agenda in 1998.There are different phases regarding how this committee dealt with the matter at hand.

Phase 1
First Steps towards Cyber Norms (From 1998 till 2004) [35]

The 1998 draft resolution was adopted as Resolution 53/70 on 4 January 1999. It built on the previous work on the Role of science and technology in the context of security, disarmament and other related fields. (A/53/576, 18 Nov 1998).

In January 2003, the Resolution 57/239, that targets the “Creation of a global culture of cyber security” was agreed upon. The next year was followed by, the Resolution 58/199, regarding the “Creation of a global culture of cyber security and the protection of critical information infrastructures.”

Phase 2
Stepping Backward, Signs of a Dynamic Process (From 2005 till 2008) [35]

The Group of Governmental Experts (GGEs) was established in 2004 to examine the threats of cyber warfare and address possible solutions. This Group was due to present a report in 2005 but ultimately failed to come to a common ground given the complexity of the issues involved.

Phase3
Forward Again. (From 2009 till 2012)[35]

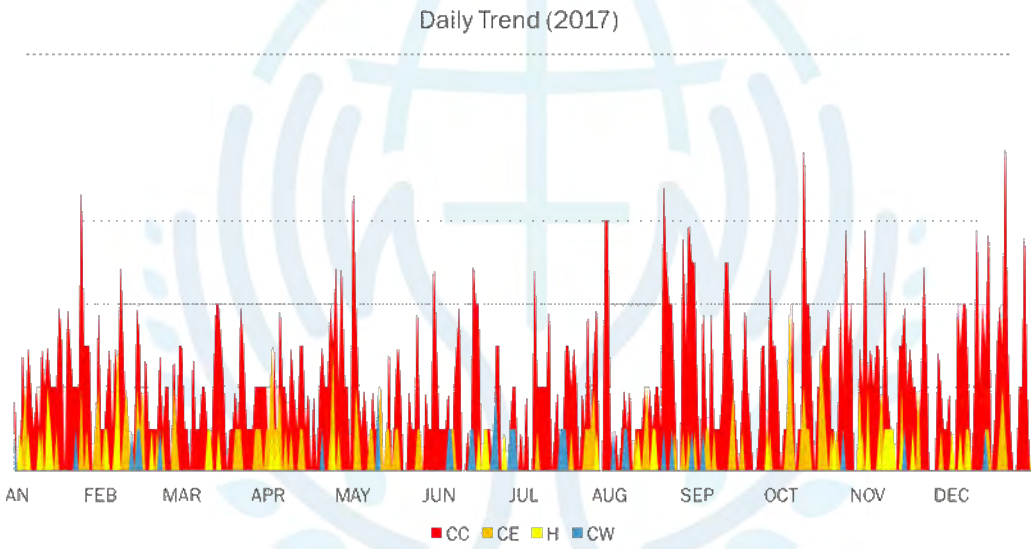
Starting in October 2009, draft resolutions in the First Committee are again adopted without a vote as during the pre-2005 period.

In 2010, the second GGE presented a report that did come to a consensus stating that: “Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century.”

In 2012, a third GGE was called upon by UN Secretary General Ban Ki Moon that presented a report tackling the clarification of which rules of warfare are applicable in cyberspace. [36]

Phase 4
Stable State (From 2013 till 2017) [35]

In 2015, GGE published a report on ‘norms, rules or principles of the responsible behavior of states in the cyber sphere as well as confidence building measures, international cooperation and capacity building’. One of which recommendation was about “Observing the principles of international law, state sovereignty and the settlement of disputes by peaceful means when using information technology.”



The graph above shows the accuracy of cyber-attacks in 2017
CC: Cyber Crime, CE: Cyber Espionage, H: Hacking, CW: Cyber Warfare[37]

Due to the unstoppable increase of cyber attacks, this committee aims to come up with a permanent solution to prevent such attacks from happening. This goes hand in hand with the duties of DISEC within the scope of the UN charter in all disarmament and international security matters.

III. Case Studies and Sub-Topics:

1. The Arab Spring: "The Twitter Revolution"

On December 17, 2010, Mohamed Bouazizi set himself to fire in front of the government building in Sidi Bouzid, Tunisia after his only resource by which he supports his mother and six siblings, his fruits and vegetables cart, was confiscated. The policewoman - claiming that Bouazizi does not own the necessary permit – confiscated Bouazizi's cart and allegedly slapped him when he tried to resist. The desperate 26 years old Tunisian's act of self-immolation was filmed by cell phones and shared on the internet leading to people's anger and protests across the country.

Within days, several protests grew around the country calling for the president that have been ruling the country for 23 years to step down and for changing the regime that lacks political freedom. The government responded by arresting people and activists in what was reported to be a brutal manner. On January 14th, amid rising violence in Tunisia, the president lfed the country, which led W what was considered the victory of the people [2].

This revolution was dubbed the "Twitter Revolution" because of the vivacious role played by social media – especially twitter - during this event. Social media turned out to be the place where people voiced their opinions and opposed corruption. Its impact lies in increasing coordination between protesters and gaining more attention to the protests. Due to this revolution, the Tunisian government took extreme measures such as hacking the social media pages of journalists and activists. To a certain extent, Mohamed Bouazizi was the trigger that led to the Arab Spring and social media was the platform to enable that.

In the Arab Spring aftermath, the uprisings in the Arab countries had different outcomes. In Tunisia, after President Zine El Abidine Ben Ali stepped down, democratic elections took place and the government underwent several institutional reforms (to increase the government's transparency and civil engagement in decision making). This led many to consider the uprising in Tunisia successful [3]. On the contrary, the Arab Spring did not bring peace, stability and transparency to other countries as it was intended. Instability caused by the revolutions in the Middle East and North Africa paved the way for violence and corruption.

2. Timeline of Some Major Cyber-Attacks

April-May 2007	Estonia was the victim of several cyber-attacks after weeks of tension with the Russian Federation. The tension between the two countries was a result of Estonia's plan to change Russia World War II memorial and move Russian soldiers' graves. The attacks disabled the internet and resulted in a complete country shut off regarding its great government dependency on the internet. Governmental offices, banks, power stations, newspapers, TV and Radio stations and other institutions were targeted by this attack. The Blackout was a Distributed Denial of Service (DDoS)* attack [4].
September 2010	Iran's Natanz nuclear facility was attacked by a malware called Stuxnet worm [5].
October 2010	A DDoS attack hit Burma few days before its first election in twenty years. The attack disconnected the country from the internet [6].
November 2010	Pakistan official governmental websites were hacked by the Indian Cyber Army [5].
December 2010	India's Central Bureau of Investigation (CBI) website was hacked by the self-proclaimed Pakistan Cyber Army in response to the Indian cyber-attack on Pakistan [5].
July 2011	SK Communications, a South Korean tech company, was hacked. This resulted in the theft of personal data (i.e.: names, email addresses, and phone numbers) from thirty five million accounts. The company traced the attack to IP addresses** in China [7].
December 2015	Ukraine was the victim of a cyber-attack on three power supply companies. According to one of the electricity distribution companies attacked, the intrusion was conducted from internet subnets*** that belong to internet providers in the Russian Federation [8]. The attack left around 235,000 houses without power [9]
September 2016	South Korea blamed North Korea for stealing the equivalence of 235 gigabytes of classified military information from South Korea including plans involving its ally, the United States. North Korea denied its involvement in this attack. The stolen documents include sensitive data like Operational Plans 5015 that guides the procedure to be implemented in case of war with North Korea and attacks against the North Korean leader Kim Jong-un [10].

*Distributed Denial of Service (DDoS): Flooding network's resources with too much data that it cannot handle, and eventually making it unavailable.
*** IP Address: A unique numerical label given to a device connected to the internet.*
**** Internet Subnet: A division of an internet network.*

3. Israeli-Palestinian Conflict

Since 1948, Israel and Palestine have been living in a conflicting status. Both countries try their best to gain people's compassion by using cyberspace. The Israel Defense Forces (IDF) use social media as a way to protect themselves and attack Palestinians. Numerous videos, tweets, and Instagram posts have been used to show how Palestine is allegedly endangering the lives of Israel's citizens and threatening the safety of the country. On the other hand, The Al Qassam Brigades,known as the soldierly wing of Hamas who began in 1986 with the objective of creating a clear military organization to stand with the goals of Hamas[32], have a very active Twitter page, where they try to reach the public by leaking sensitive photos and videos in attempts to show the misery that Israel has inflicted upon Palestine [11] [12].

As the Secretary General Jens Stoltenberg said: "Cyberwar is the battlefield of now", the ground battle between Israel and Palestine turned out to be a virtual battle that relies on social media, and where each side attacks the other via cyberspace. Many issues have risen due to this dependency on social media. The aforementioned posts which served the primary purpose of portraying the other party in a negative light created trust issues for governments, companies, and authorities who were willing to invest in both countries. The photos and news articles posted online were leading causes in turning people against each other since the citizens are lacking trust for social media posts [13].

4. First Cyber Civil War

The first Cyber Civil war started in Syria as a revolution to counter the regime that was reigning upon the country. The Syrian rebels protested against the Syrian government, and this conflict became a cyber-feud causing it to be recognized as the world's first cyber civil war. This ominous conflict has been fought out in cyberspace, where each opponent, is utilising bytes and software rather than weaponry in order to attain sovereignty on the frontline of Syrian internet.

This war shows the powerful influence cyber space has on the republic of Syria and its people, whether with the regime or not. Since May 2011, visuals were shared with the world showing the destruction that each side inflicted on the other. Those cyber actions were made to shift people's attention towards following the dominant body and oppressing those of the opposite parties [17].

The consequences of this heavy reliance on cyberspace have been real and fatal. People who were speaking illy of the Syrian government in the war were arrested by it and tortured because of personal information gleaned from their emails. Even military action plans had been retrieved via hacking, and the government's data was stolen. Eventually, the Syrian Land became vulnerable to hacking and spying attacks [14].

This cyber civil war also witnessed the birth of the Syrian Electronic Army (SEA), which is constituted of a group of hackers who targeted major news organizations and activists in the United States of America [15]. The Syrian Electronic Army has a long history of hacking websites and then taking credit for their actions to send a political message.

The actions taken by this army emerged at the turn of this decade including an attack on Forbes, Harvard University, BBC, CNN, amongst many other major publications, as they posted “fake news” and “stole data information” [16]

5. WannaCry Ransomware: World’s Biggest Cyber-Attack

In May 2017, the world witnessed the biggest and most widespread cyber-attack. The attack targeted more than hundreds of thousands of computers in around 150 countries[18]. The computer infection first appeared in India and Philippines on the 10th of May [18-19]. The WannaCry Ransomware attack, which is also called WannaCrypt, blocks control of computers until the computer user pays a ransom.

Many major companies and governmental institutions around the world were victims of that attack. Even several hospitals and health institutions were badly affected. This attack led some attacked hospitals in the UK to cancel patient’s appointments and delay some services. Recovering from the cyber infection was time and money consuming for most organizations. The expansive disruption caused by the WannaCry attack served as a reminder of the importance of cyber security and system updates. The United Kingdom security services and the US National Security Agency believed that the attack is linked to the North Korean Government related group, Lazrarus after analyzing it. This was then confirmed by grant tech companies Microsoft and Facebook along with other unnamed security community members that collaborated to take actions against the cybercrime group [19].

**Ransomware: “Software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money” Cambridge Dictionary*

6. The Islamic State in Iraq and Syria (ISIS) Use of Cyberspace for Exploitative Warfare

On 3 February 2015, ISIS uploaded a video showing a Royal Jordanian Air force Moaz al Kasasbeh, being burned to death by Islamic State extremists. Due to this killing, the Jordanian population was outraged, and so the captured jihadists were condemned to death [20].

Throughout social media, ISIS is recruiting fighters from the Western World. Around 6,000 citizens from Europe and North America have joined ISIS since 2014[21]. They were encouraging individuals to join them by either participating in their cyber war or ‘boots on the ground’ in Syria and Iraq[21].

According to the National Security Studies (INSS), the technological progress of ISIS surpasses those of al-Qaeda and other jihad movements. It is known that jihad movements such as Hezbollah, Hamas, al-Qaeda, and ISIS are all well familiar with the power behind social media particularly in exerting strong political messages. ISIS was able to utilize media exploitation at a high scale. They have shown an unparalleled rate of manipulation on Twitter and Facebook accounts showing that a new era of cyber warfare has appeared combining both physical and cybernetics jihad.[39]

ISIS has used a new technique in cyberspace by resulting in “psychological warfare”. They have drowned the internet with videos showing brutal acts of beheading and mass executions, in addition to victory parades in order to demonstrate their power and strength. In addition to that, Intel Crawler, a US Intelligence Company, has stated an increase in the spread of (NJ RAT) which is a malicious code, around the areas of Baghdad, Erbil, Basra, and Mosul. All of which are evidently related to ISIS. [40]

7. UK National Cyber Security Strategy 2016-2021

The United Kingdom is investing 1.9 billion pounds over the 5 years period from 2016 to 2021 to renovate it Cyber Security. This strategy is implemented based on the fact that the already existing cyber security plans are not enough to keep up with the fast developing cyber threats. The UK vision is that, by the end of the strategy period, their country will be "secure and resilient to cyber threats, prosperous and confident in the digital world."[38] In order to realize this vision, the UK has to implement three main objectives: Defend (make sure that all UK institutions and citizens have the capability to defend themselves in case of a cyber-threat or attack), Deter (investigating any attack targeted against the UK cyber space and prosecute the offenders) and finally Develop (having the necessary expertise and innovators in the cyberspace field to grow the UK's cyber security industry and overcome future threats). [38]

You can find more details about the UK National Cyber Security Strategy on the following
link:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

8. Some Important Focal Points

The great internet dependency of governments, institutions and the general public increases the need for safer internet. Cyber security is achieved when governments strengthen their internet observation but enhancing it may not be affordable for some countries.

The Internationals Telecommunications Union (ITU), a specialized agency of the United Nations (UN) that is responsible for issues that concern information and communication technologies reported that most countries with developing economies and less technological advancement face more cyber challenges and are less likely to have a strategy for cybersecurity[22]. According to Global Cyber Security Index

(GCI), that measures if all countries are strongly focusing on protecting cyber security [33], only 38% of countries have a cyber-security strategy and 12% have one under development. The GCI is a survey that studies country's commitment to cyber-security. The heat map in the figure below illustrates the level of commitment of countries towards cyber-security [22].

More details about every country can be found on:
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

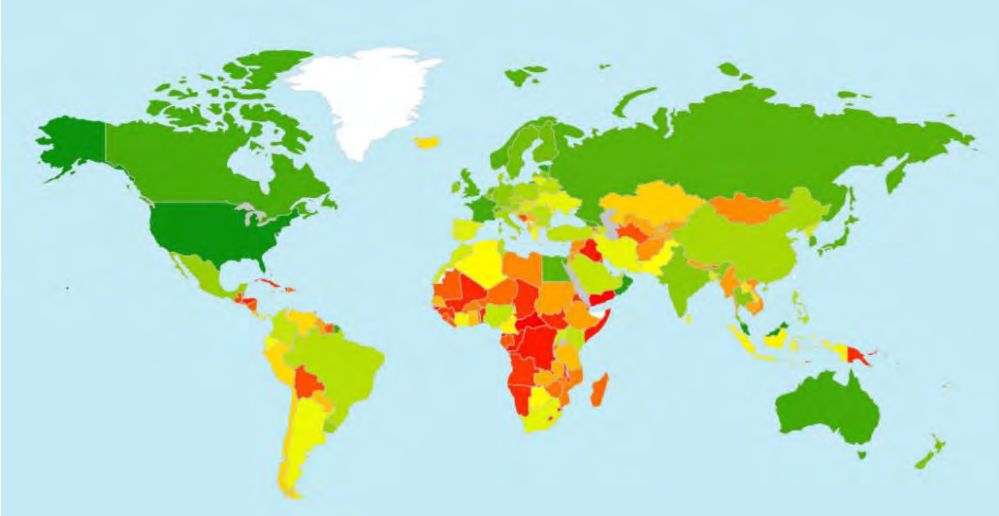


Figure above shows Countries' Level of Cyber Security Commitment (Green being the Highest and Red being the Lowest)

There was a remarkable increase in the dependency on the internet throughout the years and with the increasing number of internet users comes greater ability of spreading information. Many politicians, leaders and activists use the internet – namely, social media – as a strong tool of influence on the public. Opinions shared on the internet can have positive and negative impacts on the readers or viewers and can even incite conflicts on national and international scales.

Terrorist groups have been heavily relying on the internet and social media to gain recruits and funds. Through social media, they try to incite fear by demonstrating their power through their actions. Disturbing images, videos of hostage execution and more horrifying content is the type of media they share in order to make a statement.

IV. Additional information:

A. Treaties, Conventions and Organizations

i) IMPACT International Partnership Against Cyber Threats (ITU)[23]

ii) Convention on Cybercrime (Council of Europe, 2001)[24]

iii) 3rd annual Middle East Cyber Security Summit (March 26-27, 2017)[25]

B. Resolutions

i) Cyberwarfare a serious threat to peace and global security (Resolution adopted consensus by 132nd IPU assembly 1 April 2015) [26]

ii) General Assembly, Resolution 57/239, Creation of a global culture of cyber security (31 January 2003) [27]

iii) General Assembly, Resolution 58/199, Creation of a global culture of cyber security and the protection of critical information infrastructures (30 January 2004) [28]

iv) General Assembly, Resolution 71/28, Developments in the field of information and telecommunications in the context of international security (9 December 2016)[31]

C. The SDGs and the Topic at Hand:

The Sustainable Development Goals are a collection of 17 global goals set by the United Nations. The SDGs are all about a variety of social and economic matters that include poverty, hunger, health, education, climate change, gender equality, water, sanitation, energy, environment and social justice. The SDGs are also known as "Transforming our World: the 2030 Agenda for Sustainable Development". They were structured in order to replace the Millennium Development Goals which ended in 2015. The advantage they have over the MDG is that they involve all the countries. [41]

Reaching an economic growth and providing decent work opportunities, promoting innovation and developing the industry are a set of main goals that the SDG is aiming to achieve. But to be able to reach them, solving this matter at hand can be a step forward. Whenever the countries stop launching cyber-attacks on each other's, the trust issues may be solved and the security levels in each state will get higher. Therefore, companies and foreign governments will be encouraged to invest their money into fruitful projects that turn out to be new gates of opportunities to the citizens. Many more actions can be taken to ensure that the whole world is on the right track towards achieving most of the

goals. Peace is another achievement that can be attained if the cyber-attacks were limited and the internet was somehow controlled to filter out the information that are false specially when it comes to conflict zones.[41]

As for the goal number 16, in order to maintain an international security level, finding a solution for cyberwarfare is one way to go. Since most wars nowadays are fought in cyberspace. Conflicts between the people and the government, even conflicts between countries can rise because of a post or a visual downloaded on the internet.

V. Questions to Consider:

1. What is your government's stance regarding cyber warfare?
2. Does your country use cyberspace in its operations? If so, what is the extent of its dependence on cyberspace?
3. Has your country encountered any incident regarding cyber warfare or any problems because of social media? If so, how did it handle it? If not, were there any preventative measures taken to ensure safety and what were they?
4. Has your country been involved in a cyber-war with another country? If so, what were the consequences and aftermath of that war? If not, would your country be a spectator or active participant in the case of a war and which side might it support?
5. How does your country deal with cyber warfare and the misuse of social media?
6. What are the past resolutions that address the issue?
7. What were some of your country's national and international actions?
8. What internal policies and legislations did your nation implement to deal with cyber warfare?
9. How can DISEC prevent countries from developing their cyber warfare programs?
10. What is the role of NGOs in dealing with the current topic at hand?

VI. References

[1] Melzer, Nils. Cyberwarfare and International Law. UNIDIR Resources, 2011. Web. 1 Dec. 2017.
http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

[2] Day, Elizabeth. "The Slap That Sparked a Revolution." The Guardian (2011): n. pag. Web. 1 Dec. 2017.
https://www.theguardian.com/world/2011/may/15/arab-spring-tunisia-the-slap

[3] Botelho, Greg. "Arab Spring Aftermath: Revolutions Give Way To Violence, More Unrest." CNN (2015): n. pag. Print.
http://edition.cnn.com/2015/03/27/middleeast/arab-spring-aftermath/index.html

[4] Ruus, Kertu. "Cyber War I: Estonia Attacked From Russia." European institute.org. N.p., 2017. Web. 3 Dec. 2017.
http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

[5] Ryall, Julian. "A History of Major Cyber Attacks." The Telegraph (2011): n. pag. Web. 3 Dec. 2017.
http://www.telegraph.co.uk/news/worldnews/asia/japan/8775632/A-history-of-major-cyber-attacks.html

[6] "Burma Hit by Massive Net Attack Ahead Of Election." BBC (2010): n. pag. Web. 3 Dec. 2017.
http://www.bbc.com/news/technology-11693214

[7] Dunn, John. "Chinese Hackers Blamed For Huge South Korean Database Theft." CSO(2011): n. pag. Web. 26 Jan. 2018.
https://www.csoonline.com/article/2129187/data-protection/chinese-hackers-blamed-for-huge-south-korean-database-theft.html

[8] "The Ministry Of Energy And Coal Intends To Form A Group Of Representatives Of All Energy Companies Within The Management Of The Ministry To Study The Possibilities Of Preventing Unauthorized Interference In The Operation Of Power Grids." Ministry of Energy and Coal Industry of Ukraine. N.p., 2016. Web. 26 Jan. 2018.
http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109

[9] Windrem, Robert. "Timeline: Ten Years of Russian Cyber Attacks on Other Nations." (2016): n. pag. Web. 3 Dec. 2017.
https://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111

[10] "North Korea Hacked South's Secret Joint US War Plans – Reports." The guardian (2017): n. pag. Web. 1 Dec. 2017.
https://www.theguardian.com/world/2017/oct/10/north-korea-hacked-us-war-plans-south-korea-reports

[11] Al Helou, Youssef.” Social Media: The weapon of choice in the Gaza-Israel Conflict.” MDE (February 2015): n.pag. Web.
http://www.middleeasteye.net/news/social-media-weapon-choice-gaza-israel-conflict-1807202428

[12] Kerr, Dara.” How Israel and Hamas weaponized social media.” CNET (January 2014): n.pag. Web.
https://www.cnet.com/news/how-israel-and-hamas-weaponized-social-media

[13] Shih, Gerry.” In Israel-Palestine Conflict, Social Media Gets ‘Weaponized’.” TECH (November 2012): n.pag. Web.
https://www.huffingtonpost.com/2012/11/16/israel-palestine-social-media_n_2141862.html

[14] Ruhfus, Juliana.” Syria's Electronic Armies.” Al Jazeera (June 2015). n: pag. Press.
http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html

[15] Spark-Smith, Laura.” What is the Syrian Electronic Army?” CNN (August 2013) n: pag. Press
http://edition.cnn.com/2013/08/28/tech/syrian-electronic-army/index.html

[16] Fox-Brewster, Thomas.” U.S. Charges 3 As It Chases Syrian Electronic Army -- $100,000 Bounties On Hackers' Heads.” Forbes (March 2016). n: pag.Web.
https://www.forbes.com/sites/thomasbrewster/2016/03/22/syrian-electronic-army-hackers-charged-by-fbi/#7d73dbe50085

[17] Lee, Bryan.” The Impact Of Cyber Capabilities In The Syrian Civil War.” Fortuna’s Corner (April 2016) n:pag.Web.
https://fortunascorner.com/2016/04/27/the-impact-of-cyber-capabilities-in-the-syrian-civil-war/

[18] Thompson, Mark, and Jethro Mullen. "World's Biggest Cyberattack Sends Countries Into 'Disaster Recovery Mode'." CNN (2017): n. pag. Web. 4 Dec. 2017.
http://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/index.html

[18-19] Brenner, Bill. "Wannacry: The Ransomware Worm That Didn’T Arrive On A Phishing Hook." naked security. N.p., 2017. Web. 27 Jan. 2018.
https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/

[19] Watkins, Eli. "White House Officially Blames North Korea For Massive 'Wannacry' Cyberattack." CNN (2017): n. pag. Web. 27 Jan. 2018.
https://edition.cnn.com/2017/12/18/politics/white-house-tom-bossert-north-korea-wannacry/index.html

[20] "Jordan Pilot Hostage Moaz Al-Kasasbeh 'Burned Alive'." BBC (2015): n. pag. Web. 7 Dec. 2017.
http://www.bbc.com/news/world-middle-east-31121160

[21] “ISIS and Social Media”.OP250.Web.
https://www.operation250.org/isis-and-social-media/

[22] International Telecommunication Union. Global Cybersecurity Index (GCI). Geneva: International Telecommunication Union, 2017. Web. 5 Dec. 2017.
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[23] International Multilateral Partnership Against Cyber Threats. ITU, 2017. Web. 7 Dec. 2017.
http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf

[24] "Details Of Treaty No.185." Council of Europe. N.p., 2017. Web. 7 Dec. 2017.
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[25] "3Rd Annual Middle East Cyber Security Summit- Critical Infrastructure Information Protection." The Cyber Research Databank. N.p., 2017. Web. 7 Dec. 2017.
https://www.cyberdb.co/event/3rd-annual-middle-east-cyber-security-summit-critical-infrastructure-information-protection/

[26] "CYBER WARFARE: A SERIOUS THREAT TO PEACE AND GLOBAL SECURITY." Archive.ipu.org. N.p., 2017. Web. 7 Dec. 2017.
http://archive.ipu.org/conf-e/132/Res-1.htm

[27]” Creation of a global culture of cybersecurity 57/239.”The General Assembly (31 January 2003).Printed Doc.
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[28] “Creation of a global culture of cybersecurity and the protection of critical information infrastructures 58/199. “The General Assembly (30 January 2004)
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

[29]“Common Types of Cybersecurity Attacks: A look inside the attacker's toolkit.” Rapid7 (2017).
https://www.rapid7.com/fundamentals/types-of-attacks/

[30]“What is the Internet?”. Good Will Community Foundation (2017).
https://www.gcflearnfree.org/internetbasics/what-is-the-internet/1/

[31]” Developments in the field of information and telecommunications in the context of international security.”The General Assembly (9 Dec, 2016)
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/28

[32]"Izz Ad-Din Al-Qassam Brigades | Terrorist Groups | TRAC." Trackingterrorism.org. N.p., 2018. Web. 29 Jan. 2018
www.trackingterrorism.org/group/izz-ad-din-al-qassam-brigades

[33]"Global Cybersecurity Index." ITU. N.p., 2018. Web. 29 Jan. 2018.
www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[34]C.R., Srinivasan. "The Evolving Cyber-Threat Landscape." BWDisrupt (2018): n. pag. Web. 29 Jan. 2018.
http://bwdisrupt.businessworld.in/article/The-Evolving-Cyber-threat-Landscape/24-01-2018-138248/

[35]”General Assembly resolutions.”UN (2017)
http://www.un.org/en/sections/documents/general-assembly-resolutions/index.html

[36] “Cybersecurity: A global issue demanding a global approach”, United Nations News, 12 December 2011
https://www.un.org/development/desa/en/news/ecosoc/cybersecurity-demands-global-approach.html

[37]”2017 Cyber Attacks Statistics”Hackmageddon: information security timeline and statistics (January 2018)
http://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

[38]HM Government. National Cyber Security Strategy 2016-2021. London: Cabinet Office, 2016. Print.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[39]Tal,Koren.”Cyberspace in the service of ISIS.”INSS (Septembre 2014).
http://www.inss.org.il/publication/cyberspace-in-the-service-of-isis/

[40]Winsor,Ben.”Hundreds Of Westerners Have Joined ISIS — Here's Where They Came From.”Business Insider(2014).
http://www.businessinsider.com/isis-is-recruiting-westerners-countries-2014-8

[41] “Sustainable Development Goals.” United Nations (2015)
http://www.un.org/sustainabledevelopment/sustainable-development-goals/

Topic B
Prevention of an Arms Race in Outer Space

I. Definition of Topic:

An arms race denotes a rapid increase in the quantity or quality of instruments of military power by rival states in peacetime. This race can turn fast into a competition between countries where each one of them competes to produce larger numbers of weapons, greater armies, and superior military technology. The first modern arms race took place when France and Russia challenged the naval superiority of Britain in the late nineteenth century. [20]

The prevention of an arms race in outer space, also known as PAROS, is one of the most important issues currently under consideration by the international community. This topic is placed on the agenda of this committee to avoid any future problems regarding an arms race in space. One of the reasons this issue is critical is that satellites that are sent to orbit in space are vulnerable to damage destruction by almost anything, even the smallest materials such as space debris. According to the NASA statistics, around 500,000 pieces of "space junk" are followed as they circle planet Earth. They all move at a speed of 17,500 mph. This is fast enough for a small orbital debris to ruin a satellite or a spacecraft. [19]

Due to the lack of a general consensus between nations regarding this matter, outer space is at risk. In 2008, the draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT), was introduced to the Conference on Disarmament (CD) by China and Russia. It was a step towards the non-weaponization of space. However, this draft will not be put into action since the United States is not willing to agree on it claiming that: *"We continue to believe that there is no arms race in space, and therefore no problem for arms control to solve"*.[21]

The issue could be divided into two major categories:

Militarization of Outer Space

Militaries all over the world rely on satellites that have been launched into space since the earliest communication satellites were set free into orbit. Those satellites could be used for many different ways such as control, communication, monitoring and early warning. For example, The Global Positioning Systems (GPS) are used for navigation purposes which is classified as a "peaceful purpose", however, many people are doubtful that the use of GPS is solely peaceful. In fact, this instrument can be used as a tracking device which invade the privacy of citizens. Also, with the help of the GPS some military actions can occur such as using satellites to direct bombing raids or to orchestrate a prompt global strike capability, which is the ability to control any situation or defeat any adversary across the range of military operations. [1]

Weaponization of Outer Space

Transporting potentially destructive satellite devices into the space orbit is generally referred to as Weaponization of Outer Space. The weapons which use space as a medium to travel before hitting their targets such as hypersonic technology vehicles are also considered a part of weaponization of outer space. Tests were conducted in order to check the effectiveness of such weaponry. In 2013,the United States became the only nation known to have successfully tested the X-51A, a prototype for the planned "High Speed Strike Weapon"[24]. In addition, missiles which carry dual characteristics, meaning that they could destroy space assets, as well as other ballistic missiles* could also be deemed part of the problem. [1]

**A ballistic missile is a missile (rocket) that follows a ballistic trajectory with the objective of delivering one or more warheads to a predetermined target.*

II. Role of Committee in Current Topic:

The Committee on the Peaceful Uses of Outer Space (COPUOS) was set up by the General Assembly in 1959 to govern the exploration and use of space for the benefit of all humanity. The purpose of this committee was to ensure peace, security and development.[29]

Along with the cooperation of the United Nations Office of outer space affairs (UNOOSA),the General Assembly adopts every single year a resolution entitled *"International cooperation in the peaceful uses of outer space"* that offers valuable guidance to States on the conduct of space activities. [30]

Although previous treaties have played an invaluable and important role in consolidating a strengthened environment of international peace and security regarding the outer space, the world witnesses that with all the technological development taking place, an arm race is about to begin. That's why the UN agenda this year includes the topic at hand in order to prevent a futuristic problem.

III. Case Studies and Sub-Topics:

1. China's Space Missile Test

China launched a ballistic missile from a ground base near *Xichang Space Centre* on January 11th 2007. The missile successfully destroyed one of the Chinese aging weather satellites that it launched in 1999 - as intended - to test the missile. The anti-satellite weapon* test was conducted at 865 km above earth [2], and it created a large debris cloud (larger than any other test conducted in space before) that can damage other nearby satellites. The missile that China launched reached as high as some satellites that belong to the United States [22]. The US, Japan and Australia showed concern about the missile test that China conducted. The test underlines the growing military power of China and

the future possibility of an arms race in outer space. Later, the Chinese Foreign Ministry spokesman stated that the missile test as well as other space tests that China conducts are for peaceful purposes only, and that it opposes any kind of arms race in space.

Previously in the 1980s, both the United States and the Soviet Union conducted similar tests which they then stopped and banned such tests. However, in recent years, the US, Russian Federation and China have been working on enhancing their ASAT (anti-satellite) programs [23]. ASAT weapons can destroy satellites in low orbits, and their ground stations are more affordable and manageable than space-based missiles. This makes such kind of a space weapon a plausible one to test.

**Anti-Satellite weapon (also known as ASAT weapons) are weapons built for the purpose of targeting and destroying satellites.*

2. USSR Outer space Cannon

On January 24th 1975, the USSR (Union of Soviet Socialist Republics) fired a 23-millimeter cannon in space from one of its space stations “Salyut-3” while the cold war between USSR and the US was raging [17]. The cannon firing was revealed 40 years later in a Russian TV show (Zvezda TV) that aired a footage of this space gun, but the results of this cannon test remains classified. The R- 23M Kartech cannon was designed in the sixties to be a part of project code-named Almaz ("diamond"). The Almaz program is space program by the USSR done for military purposes during the cold war. The purpose of the cannon was claimed to be used as a defense from American space possible threats. Back then, the fear of space attacks and spying was rampant, so developing anti-satellite weapons was a logical military plan for the Soviets [3].

3. Space Lasers

In 2017, the world witnessed an altering event. China is developing a stash of first-strike space-lasers that were created for the purpose of removing space debris. [28] After sixty years of sending rockets, boosters, and satellites into space, the Low Earth Orbit (LEO) has become overloaded. Given how fast debris in orbit can travel, even the tiniest bits of junk can pose a major threat to the International Space Station active satellites. That’s why this project was designed in the first place. However, countries like the UK and USA believe that these space lasers could terminate NATO satellites, which leads to weakening the west’s ability to fight any war. [5] And the fact that China is manufacturing these lasers means that it is enhancing the weaponization of outer space. Although this may be true, China is trying to reassure other countries that these space lasers were made for peaceful purposes since China is considered to be one of the worst offenders when to comes to producing space junk. Back in 2007, China conducted an anti-satellite missile test that resulted in the creation of more than 3000 bits of dangerous debris. This debris cloud was the largest ever tracked, and caused significant damage to a Russian satellite. [28]

4. Cyber War is Space War

It is becoming clear by now that a future war between contemporary militaries can expand to the outer space and the cyber space. In fact they can both be one and the same. Due to various technological developments in the two fields, satellites operators are now able to use their radio spectrum for internet traffic, which is the main reason why experts in cyber security are worried about the convergence of cyber space and space.

Hacking satellite control communications and altering them can lead to satellite malfunction. In case hackers attacked satellites, communications, air transportations, weather monitoring and business services can face serious disruption. As mentioned before, militaries use satellites for their own peaceful purposes, however if any military actions were hacked, this could lead to world war III. [6]

In order to combat the risk of hacking, China launched the first quantum communications satellite in the world on August 2016. The forward-looking solution that China came up with is a viable option for the future for other countries as well. This kind of satellite is almost unhackable. “Once intercepted or measured, the quantum state of the key will change, and the information being intercepted will self-destruct,” Xinhua News Agency said. [7]

5. Space Debris

Besides creating a new arms race, the weaponization of space means proliferation of space debris. Space debris or orbital debris, also called space junk and space waste, are the objects in orbit around Earth. [8]

Such debris, resulting from 50 years of space activity, already poses a substantial risk to spacecraft. This crowding problem could deteriorate since a large number of space weapons could be set up in Low Earth Orbit (LEO). During a space war, if a number of satellites were to be destroyed, they would create so much wreckage that it would be kind of impossible for future satellites to be stationed in space and generally limit space access and usage. [1]

6. Relating the Topic to Today

Throughout history, man exploited every technology in military uses (e.g.: Fire, airplanes, nuclear energy, etc.). According to this logic, countries will still seek new technologies to use as weapons, and eventually space programs are among them.

Countries with a space program differ in their purposes and intentions. The reasons why countries develop a space program include – but are not limited to –weather prediction, better telephone and internet services, knowledge about space, finding alternative resources, searching for potential places for living and protection from asteroids.[25] Whereas, several countries such as USA, Russia, & China conducted experiments

and tests in the outer-space that serves military purposes. Few of these tests are represented in this background guide as case studies.

Weapons built for outer-space significantly differ in their structure, uses and dangers. Some space devices can have a dual purpose which makes a resolution for space arms race prevention more difficult. For example, satellites used for surveillance and collision prevention can also have spying capabilities and can be used for other military purposes. In November 8 2017, Morocco launched an observation satellite that was commissioned in 2013.This satellite could be used for military activities, surveillance of the borders and coastline, and monitoring desertification in the region. Yet, the launch service provider Arianespace said that: “it will be used for mapping activities, spatial planning, monitoring of agricultural activities, prevention and management of natural disasters, and monitoring of environmental developments.”[26]&[27]

Adding up to this, there is a new idea about a missile defense shield in space that came up in December 2017. This shield aims toward the deployment of missiles in space to intercept ballistic missiles. It was suggested by the United States due the testing of nuclear weapons conducted by North Korea. The National Defense Authorization Act for Fiscal Year 2018 authorizes the development of a *"space-based ballistic missile intercept layer, capable of providing boost-phase defense."* Yet, the Center for Strategic and International Studies warns about Space-based missile interceptors because of their inefficiency and vulnerability. [9]

IV. Additional information:

A. Reports and Analysis

The Conference on Disarmament, CD, established in 1979 worked on many reports [10]

i) CD/1217, Report of the Ad Hoc Committee on PAROS (1993)

ii) CD/1679, China and Russia: Possible elements of the future international legal instrument on the prevention of deployment of weapons in outer space, the threat or use of force against outer space objects (2002)

iii) CD/1844, Canada: report UNIDIR seminar "Security in Space: the next generation" (2008)

iv) CD/1925, Nigeria on behalf of member States of G-21, Working paper, Prevention of an Arms Race in Outer Space (2011)

v) CD/1941, Syrian Arab Republic on behalf of member States of G-21, Working paper, Prevention of an arms race in outer space (2012)

vi) CD/1985, Russian Federation and China: updated draft PPWT (2014)

vii) CD/2042, Letter dated 11 September 2015 from the Permanent Representative of China to the Conference on Disarmament and the Charge d'affaires of the Russian Federation addressed to the Secretary-General of the Conference transmitting the comments by China and the Russian Federation regarding the United States of America analysis of the 2014 updated Russian and Chinese texts of the draft treaty on prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects (2015)

viii) CD/2098, Letter dated 9 August 2017 from the Permanent Representative of the Russian Federation, addressed to the Secretary General of the Conference on Disarmament, transmitting the Joint Statement by President of the Russian Federation Vladimir Putin and President of the Socialist Republic of Vietnam Tran Dai Quang of 29 June, 2017, with regard to the no first placement of weapons of any kind in Outer Space (2017)

B. Treaties and Conventions[1]&[11]

i) The Partial Test Ban Treaty, formally titled the Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (1963)

ii) The Outer Space Treaty, formally titled the Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967)

iii) The Liability Convention, formally titled the Convention on International Liability for Damage Caused by Space Objects (1972)

iv) The Launch Registration Convention, formally titled the Convention on the Registration of Objects Launched into Outer Space (1975)

v) Limited Test Ban Treaty, LTBT (1963)

C. Resolutions and Agreements

vi) The Rescue Agreement, formally titled the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (1968) [1]

vii) The Agreement Relating to the International Telecommunications Satellite Organization "Intelsat" (1971) [1]

viii) The Moon Agreement, formally entitled the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979) [1]

ix) General Assembly, Resolution 65/68, Transparency and confidence-building measures in outer space activities (8 December 2010) [12]

x) General Assembly, Resolution 68/29, Prevention of an arms race in outer space (5 December 2013) [13]

xi) General Assembly, Resolution 68/189*, Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities (29 July 2013) [14]

xii) General Assembly, Resolution 70/26, Prevention of an arms race in outer space (7 December 2015) [15]

xiii) General Assembly, Resolution 70/27, No first placement of weapons in outer space (7 December 2015) [16]

D. The SDGs and the topic at hand

The Sustainable Development Goals are a collection of 17 global goals set by the United Nations. The SDGs are all about a variety of social and economic matters that include poverty, hunger, health, education, climate change, gender equality, water, sanitation, energy, environment and social justice. The SDGs are also known as "Transforming our World: the 2030 Agenda for Sustainable Development". They were structured in order to replace the Millennium Development Goals which ended in 2015. The advantage they have over the MDG is that they involve all the countries. [18]

One of these goals aims to achieve international peace and security. The prevention of an arm race in outer space is a step towards avoiding futuristic problems. In fact, conflicts can be avoided between nations if the idea of turning space into a weapon stalk is banned properly once and for all. The weaponization of outer space is a very dangerous act since anything that happens in space can threaten the peace of earth, as mentioned before space debris is one way that can affect our planet. That's why all 17 goals can be attained if countries leave their weapons away from space and focus on saving earth instead of endangering it more.

V. Questions to Consider:

1. Does the country you're representing have a space program? If so, how developed is the program compared to those in other countries?
2. How transparent is you government regarding its actions in outer space?
3. If your country has a space program, had it conducted any military or weapon experiments in the outer space?
4. What's your country's stance on outer space weaponization? Should countries have the freedom to conduct military experiments and develop weapons in space, or should the UN be responsible to regulate outer space activities to guarantee their peacefulness?
5. For what reasons a country might need to develop weapons in space?
6. How can the outer space peace be ensured?

7. How can all countries – including those with no space programs – be involved in outer space activities and informed of explorations and militarization occurring?
8. How can this conference's resolution be implemented effectively?
9. Are there any past agreements or resolutions suggested by your country regarding this issue?
10. What are the futuristic steps that should be taken in order to prevent the weaponization of outer space?
11. How do these treaties help keep space free from weapons? What do countries need to agree to in order to keep all arms out of space?

VII. References

[1] “Outer space: Militarization, weaponization, and the prevention of an arms race”. *Reaching critical will*.
http://www.reachingcriticalwill.org/resources/fact-sheets/critical-issues/5448-outer-space

[2] "Concern Over China's Missile Test." BBC (2007): n. pag. Web. 26 Dec. 2017.
http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm

[3] Zak, Anatoly. "Here Is the Soviet Union's Secret Space Cannon." *Popular Mechanics*. N.p., 2017. Web. 26 Dec. 2017.
http://www.popularmechanics.com/military/weapons/a18187/here-is-the-soviet-unions-secret-space-cann0on/

[4] Wall, Mike.” Why Asteroids Make Lousy Space Weapons” *Space.com* (4 November2011). Website.
https://www.space.com/13515-asteroid-deflection-space-weapons.html

[5] Oliphant, Vickiie. “China’s new space lasers to take out satellites leaving west at mercy of Beijing missiles” *Express* (12 March 2017). Website.
https://www.express.co.uk/news/world/778100/China-developing-lasers-destroy-enemy-satellites-futuristic-light-war-militarise-space

[6] Grant, Greg.” Cyber War = Space War.” *Military.com* (1 March 2010). Website
https://www.military.com/defensetech/2010/03/01/cyber-war-space-war

[7] Newcomb, Alyssa. "Hacked In Space: Are Satellites The Next Cybersecurity Battleground?." *NBC* (2016): n. pag. Web. 4 Feb. 2018.
https://www.nbcnews.com/storyline/hacking-in-america/hacked-space-are-satellites-next-cybersecurity-battleground-n658231

[8] “Space Debris” *Science Daily* (2017). Website.
https://www.sciencedaily.com/terms/space_debris.htm

[9] Erwin, Sandra.” New Report Slams Idea of a Missile Defense Shield in Space” *Space.com* (23 December 2017). Website
https://www.space.com/39188-missile-defense-shield-in-space-report.html

[10] “CD Documents related to Prevention of an Arms Race in Outer Space. “The United Nation Office at Geneva, UNOG (12 October 2017). Website
https://www.unog.ch/80256EE600585943/(httpPages)/D4C4FE00A7302FB2C12575E4002DED85

[11] “Treaties and agreements.” Arms Control Association (2017). Website
https://www.armscontrol.org/treaties

[12] “Resolution adopted by the General Assembly on 8 December 2010 65/68. Transparency and confidence-building measures in outer space activities” The General Assembly UN (13 January 2011). Printed Document
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/65/68

[13] “Resolution adopted by the General Assembly on 5 December 2013 68/29. Prevention of an arms race in outer space” The General Assembly UN (9 December 2013). Printed Document
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/29

[14] “Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities.” The General Assembly UN (29 July 2013). Printed Document
http://undocs.org/A/68/189

[15] “Resolution adopted by the General Assembly on 7 December 2015 70/26. Prevention of an arms race in outer space” The General Assembly UN (11 December 2015). Printed Document
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/26

[16] “Resolution adopted by the General Assembly on 7 December 2015 70/27. No first placement of weapons in outer space” The General Assembly UN (11 December 2015). Printed Document
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/27

[17]Peck,Michael.”Revealed:The Soviet Union’s Space Cannon”.The National Interest (Octobre 2015).
http://nationalinterest.org/feature/revealed-the-soviet-unions-space-cannon-14068

[18] “Sustainable Development Goals.” United Nations (2015)
http://www.un.org/sustainabledevelopment/sustainable-development-goals/

[19]Garcia, Mark. “Space Debris and Human Spacecraft.” NASA, NASA, 13 Apr. 2015,
www.nasa.gov/mission_pages/station/news/orbital_debris.html

[20]”Arms Race.”History (2009)
http://www.history.com/topics/cold-war/arms-race

[21] Jaramilo,Cesar.”In Defence of the PPWT Treaty: Toward a Space Weapons Ban.”Project Ploughshares (2010)
http://ploughshares.ca/pl_publications/in-defence-of-the-ppwt-treaty-toward-a-space-weapons-ban/

[22] Kaufman, Marc, and Dafna Linzer. "China Criticized For Anti-Satellite Missile Test." Washington Post (2007): n. pag. Print.
http://www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801029.htm

[23] "A History Of Anti-Satellite Programs." Union of Concerned Scientists. N.p., 2012. Web. 29 Jan. 2018.
https://www.ucsusa.org/nuclear-weapons/space-security/a-history-of-anti-satellite-programs#.Wm9qQqiWZPY

[24]Gubrud,Mark.”Test ban for hypersonic missiles?”The Bulletin of Atomic Scientists (2015)
https://thebulletin.org/test-ban-hypersonic-missiles8422

[25]”15 Ways the International Space Station is Benefiting Earth.“ NASA (30 October 2015)
https://www.nasa.gov/mission_pages/station/research/news/15_ways_iss_benefits_earth

[26]”Morocco launches its first spy satellite”The Defense News (8 November 2017)
https://www.defensenews.com/space/2017/11/08/morocco-launches-its-first-spy-satellite/

[27]Traboulsi,Karim.”Morocco to become space power with first ever spy satellite”The New Arab (October 2017)
https://www.alaraby.co.uk/english/news/2017/10/25/morocco-to-become-space-power-with-first-ever-spy-satellite

[28]Matt,Williams.”China Has a Plan to Clean Up Space Junk with Lasers”Universe Today (January 2018)
https://www.universetoday.com/138263/china-plan-clean-space-junk-lasers/

[29]”COPUOUS History.”UNOOSA (2017)
http://www.unoosa.org/oosa/en/ourwork/copuos/history.html

[30]”Space Law: Resolutions”UNOOSA (2017)
http://www.unoosa.org/oosa/en/ourwork/spacelaw/resolutions.html