Surf City XVIII

Huntington Beach High School

Ad Hoc on Terror

Cyberterrorism &

State-Sponsored Terrorism in the Middle East

Ashley Berdelis

Elise Bitgood

Max Milo

Welcome Letter

Dear Delegates,

On behalf of the Huntington Beach High School Model United Nations Program, we would like to welcome you to our virtual Surf City XVIII advanced conference!

Our annual Surf City conference upholds the principles and intended purpose of the United Nations. Delegates can expect to partake in a professional, well-run debate that simulates the very issues that those at the United Nations discuss every day. Both novel and traditional ideas will be shared, challenged, and improved.

It is our hope that all delegates will receive the opportunity to enhance their research, public speaking, and communication skills as they explore the intricacies of global concerns through various perspectives, some of which may be very different from their own. We hope their experiences here give them new insight and values that they can apply outside of the realm of Model UN for the betterment of the world community.

Although we will be entertaining a new style of a virtual conference, we hope all delegates will experience a fruitful and enhancing debate. Please do not hesitate to approach our Secretariat or Staff Members with any questions or concerns that you may have throughout the day. We wish the best to all our participants and hope that they may share a fulfilling experience with us! Enjoy the conference.

Sincerely,

Summer Balentine
Secretary-General

Jenna Ali
Secretary-General

Kayla Hayashi
Secretary-General

Hailey Holcomb
Secretary-General

Meet the Dias

Ashley Berdelis

Hello delegates! My name is Ashley Berdelis, and I am a senior and fourth year student in MUN. I had the privilege of attending the National High School MUN Conference in New York, where I made memories with my friends and met new people from all over the world! Aside from MUN, I am Varsity Cheer Captain, coach a middle school cheer team, and enjoy watching baseball with my family. (Go Dodgers!) I am excited to chair this conference and feel that the topics chosen are really interesting and important to address. I look forward to seeing you all in committee!

Elise Bitgood

Hi everyone! My name is Elise Bitgood and I have been in MUN for three years so far. Through participating in conferences all over Southern California, I have been able to make so many friends while educating myself about real world issues and finding out what I can do to help. MUN has also given me the opportunity to grow in my public speaking and researching abilities, two skills that I know I will use for the rest of my life. Other than MUN, I am quite interested in fashion and spend a lot of my time at thrift stores or flea markets looking for pieces I can fix up. I love to sew and am always in the process of creating something, whether it be a shirt, hat, or bag. When I'm not doing this, I enjoy hanging out with my friends and exploring new places. I can't wait to see you all in committee and hope you all enjoy the conference!

Max Milo

Hey delegates! I am Max Milo, and this is my 3rd year in MUN. I love tackling topics about everything from technological innovations to international conflicts. I've met a lot of good friends at conferences, and they're a fantastic place to practice important life skills. In my spare time, I enjoy reading, playing video games, and listening to music. One of my favorite pastimes is sleeping. I'm on the school soccer team, and I play for a club as well. I volunteer for Link Crew and National Honor Society, helping those around me and the environment whenever I can. My dog is my life. We are going to have an exceptional time in committee!

All Papers are due on January 2, 2021 by 11:59pm to surfcity.adhocterror@gmail.com

TOPIC 1: "Cyberterrorism"

BACKGROUND

In the 1970s, a BBN Technologies engineer coded a program capable of hopping between computers connected to the ARPANET, the predecessor of the modern internet. Nicknamed the "creeper," the virus filled the screen with a taunting message. A friend of the engineer later coded his own program—unknowingly creating the first antivirus—that not only hopped from computer to computer but also deleted the "creeper" virus upon discovery, earning the name the "reaper." The "creeper" caused little harm to the computers it infected but led the way for a future full of malware[1]. The first instance, a denial-of-service attack, came in 1989[2]. The subsequent Morris Worm affected 10% of all computers connected to the internet, drastically slowing processing speeds through exponential self-multiplication until a system crashed. Eventually, the entire internet was shut down, and Morris himself was charged with computer fraud and abuse. At the time, cybersecurity lacked the proper resources and knowledge to effectively deal with easily eradicated viruses like the Morris Worm[3]. Thus, Computer Emergency Response Teams (CERTs) and antivirus software quickly became necessities in the 1990s.

As expected, cybercrime and cybersecurity constantly evolve and change in reaction to and preparation for the other. Cyber attacks are conducted utilizing a wide variety of malware, maleficent software made to damage and disrupt. While media frequently refers to most malware as a type of "virus," computer viruses only account for 10% of all malware. A virus modifies the code of a program, ensuring that activation of said program results in both the activation of the virus and its duplication. To this day, a virus is still incredibly difficult to remove, and antivirus software usually just deletes the infected program. Yet, the development of much more effective malware has caused a decline in the popularity of the computer virus. The worm, which replicates like the virus, poses a much greater danger as it requires no user interaction for activation. Simply opening an email could lead to the exponential growth of worms on a network. Trojans contain harmful code amongst the original lines and appear to be accepted and secure programs but require activation. Cyberterrorism is built on ransomware. This type of malware encrypts multitudes of files, only opening them if an untraceable cryptocurrency ransom is paid. Adware is usually harmless, only distracting and frustrating the user with pop-ups and redirects. Spyware enables hackers to spy on users and systems, obtaining passwords and personal information, but is easily removed. File-less malware must be taken more seriously. Traveling through tools built into an operating system, file-less malware is harder to detect and remove. Unfortunately, all of the aforementioned items can be combined to create even more dangerous cyber attacks: virus-Trojan-worm combinations for instance[4].

Denial of service (DoS), inciting terrorism online, and phishing are all part of the cyberterrorism arsenal as well. Phishing attacks involve spam emails containing malware sent to large numbers of potential victims. While 52% of all breaches involve hacking, a third involve phishing attempts. Emails with .doc, .dot, or .exe attachments account for 56.5% of phishing attempts. 94% of all malware is delivered by email. 62% of businesses saw phishing and social engineering, a cyber attack relying entirely on a user willingly giving up valuable information, attacks in 2018. In fact, only 5% of the average company's information is properly protected.

The worldwide information security market is projected to reach $170.4 billion in 2022, and the potential for the cyber security industry is growing exponentially[5].

After the Morris Worm, cyberterrorism grew at an alarming rate. “Sniffer” spyware at a US Air Force research facility compromised over 100 acouunts in 1994. In 1999, a 15 year old stole a piece of NASA software through a backdoor, causing a 3-week long shut-down of all systems. In 2000, a Russian hacker extorted $1.4 million from CD Universe, and a different 15 year old led DoS attacks on Amazon, CNN, eBay, and Yahoo!, causing $1.2 billion in damages.[6] 2000 marked an incredibly significant time with the emergence of the ILOVEYOU virus. Fifty million computers were affected in almost every country. Originating in the Philippines, ILOVEYOU took five hours to spread from Asia to Europe to North America. The United Kingdom’s House of Commons, Denmark’s Parliament, Ford Motor Company, Microsoft, AT&T, and the US Pentagon were all forced to take systems offline. A fairly poorly coded couple of lines, ILOVEYOU’s baffling spread was in the name. Intrigued by a potential “love letter,” users all over the globe clicked into the email, providing all the interaction necessary. The virus quickly replicated and emailed itself to every single contact on the hosting device, and the recipients soon fell victim to the virus upon opening the email. However, ILOVEYOU’s source code had an additional task. Following infection, the virus climbed around a device’s hard drive, from file to file, renaming and deleting at a rapid pace[7].

ILOVEYOU brought to light the importance of not only cybersecurity but public awareness as well. The virus itself was easily traceable and detectable, but human ignorance allowed its rapid spread. Built in 1995, secure sockets layer enabled safer money transactions on the internet, leading to the development of HyperText Transfer Protocol Secure (HTTPS) later on. Legislation like the Gramm-Leach-Bliley Act (GLBA) placed restrictions on the methods companies could use to collect personal data of subjects and led the way for modern day infrastructure like the General Data Protection regulation (GDPR) or the Cybersecurity Act[8]. The GDPR, passed by the European Union, dictated that any company accessible online in Europe must maintain complete transparency with data subjects or face a fine of either €20 million or 4% of their global revenue—whichever is largest.[9]

In recent years, cyberterrorism has grown beyond individual efforts. Organisations of cyberterrorists have emerged alongside government hackers. Estonian banks were sporadically attacked in 2007, allegedly by angry Russian activists[10]. In 2010, over 25 individuals, all part of an Eastern European cybercrime ring, were charged for the theft of $70 million from US banks. Groups of hackers stole 100 million credit card details from Sony’s data storage records, compromised millions of email addresses in an attack on JP Morgan Chase, and exposed the information of over 35 million South Koreans all in 2011. Named the “Global Bank Hack,” an attack on over 100 institutions across the globe lead to a successful £650 million theft over a span of 3 years[11]. The Stuxnet worm, claimed to have been created by Israeli and American hackers, infected hundreds of millions of computers silently. Stuxnet continued to hop from computer to computer until landing on the Iranian nuclear power plant system and wiping out multiple centrifuges[12]. “Red October” was detected in 2012 after 5 years of successful snooping. The virus obtained valuable information from government embassies, military installations, nuclear infrastructures, energy providers, and research firms.[13] 2017’s ransomware WannaCry affected 150 countries, asking for $300 per computer[14].

Cyberterrorism covers a broad spectrum of crimes, affecting virtually every nation. In the past 4 years, security breaches have increased by 67%, and 1 in 13 web requests lead to malware. These cybercrime damages are projected to reach $6 trillion annually by 2021[15].

UNITED NATIONS INVOLVEMENT

In 2011, Resolution 65/230 requested the Expert Group to Conduct Comprehensive Study on Cybercrime and determine what regulations and laws can strengthen the response to cyberterrorism.[16] The Expert Group has evaluated many regions, taking into account national legislation, best methods, technical assistance, and cooperation, in order to propose feasible and effective responses. It has been used since and has been commended for its work and seeks continuation of its work in numerous resolutions. For example, Resolution 26/4 (May 2017) decided the Expert Group needed to focus on certain areas, including legislation and frameworks, criminalization, law enforcement and investigations, electronic evidence and criminal justice, cooperation from the international community, and prevention.[17] The Expert Group also works in coordination with the Global Programme on Cybercrime, which helps countries with capacity building and technical assistance to combat acts of cyberterrorism. The Global Programme on Cybercrime wants to prosecute those who carry out cybercrime in an effective way, create better communication between nations, and increase public knowledge on the subject.[18] In December of 2019, Resolution 74/247 decided to open an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes that would consider all that has been done and all information acquired, especially the findings of the Expert Group.[19] The committee was supposed to meet in August of 2020 for a three day session to agree on how to proceed, but it was cancelled due to the situation with COVID-19 and rescheduled to March 2021.[20]

In 2017, the United Nations Office on Counter-Terrorism (UNOTC) was established by the General Assembly. The UNOTC has set many initiatives to combat cyberterrorism in light of new technologies. The Cybersecurity and New Technologies Programme has focused on prevention and monitoring the threats, misuse of technology by terrorists, and impacts of cyberterrorist attacks. They have attempted to use social media to gather proof and collect information on online terrorism, while honoring Human Rights.[21] The UNOTC's UN Counter-Terrorism Centre (UNCCT) collaborated with the Office of Information and Communication Technology (OICT) to create the Cybersecurity Challenge. This #CyberChallenge event took place December 5, 2019 in Vienna, Austria.[22] The goal of this event was to establish a solution in one of the four areas of digital terrorism, including financing, communication, cyber-kinetic attacks, and spread of online content. In addition to the solutions agreed on, the event determined that the youth is vital in prevention methods, as they are more vulnerable and targeted for attacks, but that this information from attacks could be useful in developing effective prevention methods in the Innovation Challenge.[23] The Innovation Challenge will target certain regions of Asia and Africa.

The Security Council passed Resolution 2341, which urges nations to have coordinated efforts and develop strategies to reduce the risks from the attacks, including raising awareness, preparing for attacks, and responses for security and consequence management. This resolution passed in 2017 also encourages investigation and disabling infrastructure critical to attacks, like logistics, planning, training, and financing.[24]

CASE STUDY: Russian Cyber Terrorism

Coming in the form of cyber attacks, Russia has taken part in cyberterrorism for the last two decades, starting with its ongoing interference in the Baltic States, and more recently with its engagement with Ukraine.[25] Russia has participated in espionage and sabotaging of eastern nations for decades, but it was only recently that Russia moved their efforts to the cyber sphere, a way of damaging countries without being directly tied to or accountable for the attacks. In the last five years, Russia has conducted several cyber attacks that have targeted everything from Ukranian power grids to governmental infrastructure databases. These attacks are classified as cyberterrorism as they are widely speculated to be controlled by Russia, but Russia has yet to acknowledge or confirm any of the attacks.

The first major breach of Ukraine's cybersecurity occurred in 2015 on December 23rd, during which hackers were able to get into control centers of three separate electricity systems and disable SCADA systems, allowing the malware to then reach 30 smaller centers across the country and using breakers in order to prevent these regions from getting power. As a result of this attack, over 200,000 Ukrainian citizens living in the Ivano-Frankivsk region as well as the capital of Ukraine, Kiev, lost access to power. Again in 2016, malware took the same actions on Ukraine, this time only hitting one station in Kiev, but nevertheless showing the control and ability that Russia ultimately had over Ukrainian power systems. In this case, like many others, it is extremely difficult to prove the origins of cyber terrorism, as hackers are often disconnected from any form of government or group and remain 100% anonymous.

Russia had several motivations for these attacks and the ones that they continue to ensue currently. Like other previously annexed eastern european nations, Ukraine has, in the last decade, worked toward eliminating its dependence on Russia through increased relations with the European Union and support from NATO not only politically and economically, but also militarily. As well as this, Russia is aware that many countries, especially ones that are in slow stages of growth such as Ukraine, have a lack of cybersecurity measures and therefore do not have any way to respond or retaliate to attacks on their online infrastructure. The 2016 attacks are widely seen as not done for any political or economical gain, but instead as a threat to Ukraine in order to instill fear among its people and reinstate the indirect control and authority Russia had over Ukraine despite its recent movement toward independence from Russia and it's working more closely with the European Union.

Although many countries and bodies have attributed the attacks to Russia, it was unclear who exactly was in charge of the attacks, but several Russian cyber-criminal groups are suspected.[26] Recently after the 2015 attacks, Ukraine uncovered audio recordings of those behind the attacks and announced they were Russian-speaking, and the content of the recordings led Ukraine to believe the attacks might have been headed by Advanced Persistent Threat 28 (APT28), a cybercrime group far from new that had also been blamed for collusion with the Russian government as well as interference in several countries such as with the Ukrainian Election Commission, the Pakistani Military, and the United States Democratic National Committee.[27] However, at a later meeting between Ukraine and the United States, attended by its power industry executives and leaders, the US announced that one of the accessed companies had indeed been reached through Russian internet networks, taking the blame off of APT28, and leading the investigation toward groups such as the SandWorm Team, who had in the past targeted NATO and other European nations. SandWorm is infamous for using the "BlackEnergy3" malware which was attributed to the hacking of the energy grid.[28] Later, in 2017, the Ukrainian government worked with the private online security system Dragos in order

to further investigate, which ultimately resulted in the further blame on SandWorm for the attacks.[29]

SandWorm has had a history of large-scale cyber attacks which have gotten more and more elaborate as time passes. Groups like SandWorm are usually hired through the black market by governments in order to conduct specific operations, but are not monetized and therefore are even harder to uncover than usual on the black market.[30] SandWorm has been attributed to many severe attacks in the past, including 2007 Distributed Denial of Service (DDOS) attacks, which were extremely successful because of the diverse strategies used by the team to control software. In this attack, SandWorm was able to easily access lockdown software through spear phishing emails which contained attachments that allowed hackers into the secure internet system. In addition to this, SandWorm has also been known to use malware that automatically strips and wipes computer systems of data and prevents them from being able to reset. Techniques like this make it easy for hackers to harvest private VPNs, giving them control of entire systems of data that otherwise could only be reached through individual hacking.[31]

Sources have also stated that SandWorm continues to make malware developments and advancements that will enable them to prolong blackouts and take further control of regions in the future. The efforts of Russia on ex-soviet nations have proved the control and influence that Russia has over the cybersphere, and some have even claimed that these eastern nations along its western border are only a testing ground for Russia and what it will do to other nations on a larger scale.[32] The increase in the use of cyberterrorism by Russia and Russian cybercrime groups has resulted in what is classified as cyberwarfare, a modern type of warfare in which traditional war tactics are used as well as cyber attacks.[33] Cyber warfare is a very probable thing of the future that is almost inevitable as our society moves toward more complete dependence on internet based infrastructure, and will undoubtedly happen once other countries start participating in cyberterrorism as well.[34]

While hybrid warfare could be considered low intensity compared to traditional warfare, when perpetrated and engaged in between various nations, hybrid warfare will undoubtedly grow to be high-intensive and has the potential to affect entire national population's.[35]

Russia has over and over claimed that its position on cyberwarfare is only a position of defense and they have publicly stated they have never been behind a cyber attack in not only public conferences but also in their national doctrines. Cyberterrorism is a certain way for countries like Russia to assert dominance on their neighbors without receiving much attention from organizations like NATO and the international community as the attacks remain factually anonymous. Although Russia is one of only several countries accused of cyber attacks and participating in cyberterrorism, it can be assumed that other countries on its level are working toward the same capabilities and if provoked might engage in the same actions. Overall, Russia's speculated cyberterrorism based attacks on Ukraine prove the potential danger for nations all over the world while exemplifying the lack of cyber security precautions that make nations so vulnerable to danger in the cybersphere.

QUESTIONS

1. How has your country been affected by any type of cyberterrorism, cyber attacks, or cyber warfare?
2. What are the needed precautions that countries should take in order to prevent being affected by cyberterrorism and should countries retaliate when attacked through the cybersphere?
3. The ILOVEYOU virus caused an estimated $10 billion in damages because of human curiosity at a potential love letter[36]. How would educating the public on cyberterrorist attacks be a necessary action to defeat cyberterrorism?
4. How could governments monitor or protect their technology systems in order to prevent major destruction from attacks?
5. What role does the black market serve in addressing the issue of cyberterrorism?
6. Terrorism in general is difficult to define. The think tank International Centre for Counter-Terrorism has amassed a over 260 definitions of "terrorism" from universities, NGOs, and governmental bodies across the globe[37]. The *Routledge Handbook of Critical Terrorism Studies* argues that people, governments, and organizations tend to define terrorism as "violence [they] don't support[38]." Why is an internationally accepted definition of terrorism so hard to obtain, and how would this definition affect the actions and policies of nations?

TOPIC 2: "State Sponsored Terrorism in the Middle East"

BACKGROUND

By definition, state-sponsored terrorism is terrorism conducted by private extremist groups that are supported by the government of a given country or acts of terrorism carried out by a country's government. Most of the time, governments sponsor terrorism by funding groups efforts as a result of corruption in the government which has lead to an alliance between terrorist groups and the governing bodies of nations.[39] More specifically, sponsoring of terrorism by a state can include financial aid, provision of weapons and or space, and help in the organization, planning, or conducting of operations. Currently, four countries in the world are labeled as state sponsors of terroism including the Democratic People's Republic of Korea, Iran, Sudan, and Syria.[40] Iran is considered to be the most forthcoming sponsor of terrorism, as it has been designated as a sponsor of terrorism by the United States since 1984. Terrorist organizations that are currently supported by states in the middle east include but are not limited to Hamas, Hezbollah, and the Palestinian Islamic Jihad. An example of long-standing state sponsor of terrorism is Iran, which has supported Hamas and Hezbollah, groups that are both anti-Israel, for years. Iran supports these groups because they carry out actions that fit it's policy toward Israel.[41] Countries also provide support to terrorist groups by providing places for them to hide and giving them so-called "safe havens," such as when Sudan allowed the known leader of Al Qaueda, Osama Bin Laden, to hide within their borders after he was expelled from Saudi Arabia.[42]

According to Amnesty International's estimates, around one hundred countries today participate in terrorist activities against their citizens, which can range from torturing and or jailing people that have different views or beliefs from the government, to sponsoring assination groups who seek out specific people that the government wants to get rid of.[43] Countries who engaged in this type of terrorist include but are not limited to Brazil, Columbia, Peru, Guatemala, Honduras, and Sudan. Specifically in the middle east, Iran was infamous for hunting down activist figures who disagreed with their policies and jailing or killing them in order to make sure they did not gain followers and their stances did not become popular among other people in the country.[44] Genocide is another form of state-sponsored terrorist, which has not yet happened on a large scale in middle eastern countries.[45]

As an example, Iran has been called the worst perptrator of terrorism and is said to be the government that supports terrorism on the largest scale.[46] In 1979, the current leader of Iran at the time, Mohammad Reza Shah Pahlavi, was forced to flee and his position was taken over by Ayatollah Ruhollah Khomeini, who did not favor the United States like his predecessor had. For this reason, under his term, Khomeini allowed mobs and crime organizations to take over the US embassy in Iran and hold people there hostage for hundreds of days. This was Iran's first major governmental terrorism based action that would set the precedent that actions like these were allowed under the Iranian government. Not long after this, Iran began looking to other countries and regions with hopes of setting up Muslim governing bodies similar to theirs. To get this accomplished, Iran turned to terrorist groups to carry out their actions, thus allowing Iran to accomplish their goals without any direct blame placed on them, which helped them receive less

negative attention from the international community.[47] According to the United States and it's many ally countries, Iran has been committing terrorist acts through both it's Ministry of Intelligence and Security and it's Revolutionary Guard Corps, Iran's main militant group.

Similarly, Iraq has also been long accused of supporting terrorism both within it's government and through private groups. Since 1991, the United Nations has been suspicious about offensive actions taking place within Iraq's governmental bodies, and for this reason they sent UN based inspectors, who were successful in finding both chemical and biological weapons that the Iraq government had denied having. Later in 2001, the Iraqi government was still denying access for UN inspectors to inspect their offensive infrastructure, leading the UN to accuse them of hiding arms. One reason that Iraq would be so adverse to the UN knowing about their possession of these weapons is because they were planning to use them internally in acts of terrorism against their own people. Allegations have also been put on the Iraqi government for threatening to kill it's people that had fled to Europe as well as their relatives who still remained living in Iraq. Furthermore, Iraq also publicly hosts terrorist groups within their border including the MEK, the Palestine Liberation Front, and the Abu Nidal Organization.[48]

Syria is another main sponsor of terrorism in the middle east, which can mainly be attributed to it's wishes to destroy the Jewish State.[49] Although Syria has supported various terrorist groups in the past including the Popular Front for the Liberation of Palestine- General Command (PFLP-GC), the Popular Front for the Liberation of Palestine (PFLP), and the Palestine Islamic Jihad (PIJ), several still have their headquarters located in the capital of Syria, Damascus.[50] In the last few decades, Syria has however decreased it's support for terrorist organizations, but there is still a lot to be eliminated.

Another reason states may engage in terrorism is to ensure election outcomes or to suppress political opponents that pose a threat to the ultimate control they have over their poeple. However, there is discrepancy between what is considered state sponsored terrorism and what is considered a part of a totalian government, which many governments in the middle east are. While it is debated country to country what is considered a crime and is guilty of jailtime and torture, the main deciding factor in whether a country is a perpetrator of internal terrorism is if they give their people trials, many of which do not.

In many of these instances, it can be seen that sponsored terrorism was ensued after a corrupt political figure rose to power or a militant group became to strong in the given country so that it was able to override judicial laws and conduct actions without any repercussions from the mainstream government. Overall, many large scale terrorist groups are or have at one point been supported by governments who give them the resources and means to keep committing harmful actions. Because much of terrorism depends on resources from governments, halting state sponsored terrorism in the middle east could greatly decrease terrorist acts committed globally and could get rid of the fervent power handle terrorist groups have on specific regions of innocent people. The main aspect of stopping state sponsored terrorism is ending corruption within governments that perpetrates unlawful actions and allows extremist groups to be funded, which is mostly the result of corrupt leaders that rise to power in these states and gain power and a following through instilling fear in their people and anyone who chooses to go against them. Although it has been going on for centuries, state sponsored terrorism still poses an immense threat to people around the globe and must be eliminated at all costs.

UNITED NATIONS INVOLVEMENT

The UN has created hundreds of resolutions on terrorism since turn of the century. This great increase can be directly attributed to the establishment of the Ad Hoc Committee on International Terrorism at the 1996 27th session of the General Assembly. Containing 35 members, the Ad Hoc was created to usher in an international convention for the suppression of terrorism globally[51].

In 2001, the UN Security Council unanimously adopted resolution 1373 following the September 11 terrorist attacks on the United States. This resolution established the Counter-Terrorism Committee (CTC) to implement the listed operatives. The CTC was tasked with criminalizing the financing of terrorism as well as the encouragement of asset freezes as a punishment for relation to terrorist activities. The prohibition of terrorist safe havens and criminalization of passive assistance to terrorism was also included. The CTC also encouraged international cooperation and sharing of information on any planned attacks, detailing cooperation in investigation, arrest, and prosecution. In 2004, the Counter-Terrorism Committee Executive Directorate (CTED) was established to aid the CTC in coordination in Security Council resolution 1535[52].

The most widely-referenced program emerged in 2006. Created by A/RES/60/288, the UN Global Counter-Terrorism Strategy is the main source for internationally-accepted terrorism regulation. The Strategy consists of 4 pillars. Member States must address conditions allowing the occurrence of terrorism domestically. Preventative and combative measure must be taken against said terrorism. The UN must help Member Nations strengthen their abilities to counter terrorism. Finally, the respect of human rights for all is a rule of law and an integral player in the fight against terror. The same resolution reviewed previous counter-terrorism strategy, examing A/72/840 and A/RES/72/284 and conducting five reviews[53].

A 2005 Security Council resolution, S/RES/1624, called on Member States to criminalize protecting terrorists. The resolution simultaneously called for an enhanced dialogue on state-sponsored terrorism, leaving the responsibility of procuring and fostering said dialogue on the CTC[54]. Resolution 2178 of 2014 called for states to seek out and eliminate domestic connections to terrorists, tracing and halting funds. The CTED also recognized the potential difficulties for some nations in attempting to freeze assets with limited resources[55]. In 2019, the UN Security Council unanimously adopted resolution 2462, reaffirming resolution 1373. This resolution urged nations to ensure their laws allow prosecution of any collection of funds for terrorist activities. The Council went on to caution Member States, reminding them to also ensure domestic laws abide by international human rights law, even while dealing with prosecuted and convicted terrorists[56].

In 2002, an incredibly significant arms embargo was placed on Iran through S/RES/1390. The Security Council also requested a report on all measures taken against terrorism by Member States[57]. The next major restriction on Iran came in 2008. S/RES/1803 authorized nations to search Iranian cargo should the specific government feel justified in doing so[58]. S/RES/1989 created the ISIL and AL-Qaida Sanctions Committee in 2011, yet another step toward enforcing restrictions on states harboring or providing passive assistance to terrorists[59]. In 2015, S/RES/2258 called on neighboring states of Syria to restrict the flow of terrorists in and out of Syria, noting the passive assistance of the nation in question[60]. A few months ago, the US introduced the “Commonsense” resolution. While it has not been voted on yet, many Member Nations agree with the policy and prospective actions of the document. The “Commonsense”

resolution extends the 13 year old arms embargo on Iran, claiming it cannot be lifted until Iran is free of terrorist activity[61].

CASE STUDY: Syria

Since December 29, 1979, the United States has declared Syria a state sponsor of terrorism because Syrian support for Palestine terrorism was viewed as a cause for concern.[62] With the declaration, the U.S. placed economic sanctions on Syria, which after a while caused a huge strain to their economy and the benefits enjoyed in the 1970s vanished. Syria has supported numerous terrorist organizations in the past, including the Popular Front for the Liberation of Palestine- General Command (PFLP-GC), the Popular Front for the Liberation of Palestine (PFLP), the Palestine Islamic Jihad (PIJ), the Islamic State of Iraq and Syria (ISIS), Hamas, and Hezbollah. Syria has been known to continually support terrorist groups by political and military means, especially by providing safe havens.

The Soviet Union provided security and stability in Syria, seeing as Syria was one of the USSR's only reliable allies in the Middle East.[63] For this reason, when the Soviet Union was destroyed, Syria became a center for terrorist organizations like Al-Qaeda and later ISIS. With no stability from the USSR, Syria desperately needed a strong, powerful leader for them, which ended up stemming from terrorist organizations such as Al-Qaeda. Al-Qaeda was able to provide a substantial amount of aid to Syria.[64] Once it turned into ISIS, the Islamic State of Iraq and Syria, was very involved in Syria. ISIS has been defeated before in 2010, but by 2013 they had expanded from Iraq to Syria. In 2015, ISIS was making about one to two million dollars in oil sales each day, and it was estimated that about 44,000 barrels were produced in Syria per day.[65] A portion of the money did go back to Syria, which serves as another incentive to continue to support the organization. This brings about more economic reasons for sponsoring terrorism, as Syria would not be better off without the money. As previously mentioned, Syria is a very dependent country. The U.S. economic sanctions that continue today (and through the Civil War) do not help Syria's financial standings either.[66] At one point, ISIS even had almost eighteen thousand square miles between Syria and Iraq, not including twenty thousand square miles elsewhere. 2015, however, was the peak of ISIS, as the terrorist organization lost their territorial foothold in Syria in 2019. The U.S. had captured ISIS leaders, and Turkey would be responsible for captured ISIS people. Having the Turkish in charge poses questions as to how permanent the loss of location in Syria will be.[67] External help was and is necessary from getting ISIS out of Syria, and it shows proof that international support can be an effective solution to dissolving terrorist groups and getting them out of countries.

Syria and Hamas, a terrorist group that supports the Palestine national movement, have also had a long relationship with Hamas. In 2001, Hamas set up headquarters in Damascus, Syria after the nation of Jordan expelled their leaders. While Syria only lets the organization have a safe haven in the country and no financing or logistics, this is still a way of supporting terrorism. Syria supports Hamas because it gives Syria a sense of legitimacy within the Arab nations and makes sure that Syria will not be left out in any settlement between Israel and Palestine, which is a concern to them because they share borders with Israel and Lebanon and has interest in how it will turn out.[68] Syria also allowed weapon shipments to pass through their country. For example in March of 2011, fifty tons of smuggled weapons from Iran were intercepted on its way to

Hamas. Although Syria never gave financial assistance to Hamas, they did allow money transfers to the Palestinian Authority from the Syrian national banking system. However, Syria and Hamas lost ties once the Syrian Civil War began because they would not express support for President Bashar al-Assad's side. For this reason, Hamas moved their headquarters to Doha, Qatar resulting in their public support for the rebels in 2012. Recently, Hamas has attempted to move their headquarters back to Damascus, and they want the return to occur on their own terms because they believe that the Syrian government is weaker. The terrorist organization thinks that if they can be open to Iran and Russia being main supporters to the regime, then they will be more accepted to come back into the country.[69]

Hezbollah, a Lebanon based political party and militant group, has a large presence in Syria., including twenty-eight locations that were deployed in 2019 and another thirty where there is a presence of cells which operate under the Golan Project. The Golan Project is a network in the Golan Heights on Syria's side that is designed to carry out attacks on Israel.[70] Even though commanders of the Southern Headquarters located in Syria are Lebanese Hezbollah, the troops that are militarily trained all consist of all local Syrians. Not all Syrians join for the same reason: some do it because of their military background, but others do it for financial reasons who are local villagers in the area. Cells from the Golan Project and Southern Command have already taken action through attacks against Israel, who aims to prevent Hezbollah from occupying the Golan Heights.[71] Israel had formally captured the Golan Heights from Syria in 1967 as a result of the Six Day War.[72] In fact, the Hezbollah head of operations has already killed U.S. troops that were in Iraq. In relation to assisting Syria, Hezbollah has helped President Bashar al-Assad regain control in areas of rebel territory throughout the Syrian Civil War. Prior to the Civil War, Hezbollah operated at a limited scale in Syria.[73] That being said, Syria and Hezbollah have had a relationship since the 1980s, and it grew stronger when the Lenanese Civil War ended in 1990. Hezbollah has worked hard to preserve their relationship with Syria ever since. The Syrian Civil War was seen as an upperhand to Hezbollah, which was seen as exploited through opening the Golan Project. Since 2015 however, President Assad's regime has used Russian military resources to rebalance the relationship.[74] Doing this was also a way for President Assad to stay in power, since Russia plays a crucial role in this.

Overall, Syria has supported and continues to support multiple known terrorist organizations. It is clear that there are numerous reasons for this support. First, there are political reasons, for President Assad has needed the assistance. Much of this can be attributed to the Syrian Civil War, with the Assad Regime trying to do as much as they can to keep in power. Secondly, there proves to be great financial incentive to support terrorist organizations. Syria tends to sponsor pro Palestine organizations, which helps their standing with the other Arab nations. There are also less hands on ways that Syria has sponsored terroism, such as providing safe havens and allowing shipments to pass through the territory. Either way, it is important that the issues related to state-sponsored terrorism in Syria to put a stop to it.

QUESTIONS

1. Does your country support any terrorist groups or engage in any form of terrorism toward it's people? If not, is your country working to suppress terrorism in other countries?
2. How can corruption within governments and through government officials be eliminated?

3. How can we address state-sponsored terrorism without infringing on a nation's sovereignty?
4. How can poorer nations that lack sufficient resources effectively combat terrorism on a domestic level to avoid unintentional passive assistance?
5. How would persuading or incentivising nations that sponsor terrorism to cut ties with terrorist organizations be effective?
6. How can the international community protect citizens from state-sponsored terrorism governments from becoming affiliated with terrorist organizations?

Endnotes

1. www.techopedia.com/definition/24180/creeper-virus
2. www.britannica.com/technology/denial-of-service-attack
3. https://www.herjavecgroup.com/history-of-cybercrime/
4. https://www.uscybersecurity.net/malware/
5. www.varonis.com/blog/cybersecurity-statistics/
6. https://www.herjavecgroup.com/history-of-cybercrime/
7. https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html
8. https://cyberexperts.com/history-of-cybersecurity/
9. https://gdpr.eu/what-is-gdpr/
10. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm
11. https://www.herjavecgroup.com/history-of-cybercrime/
12. www.fortune.com/2018/05/12/cyberwar-cyberattacks/
13. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm
14. https://www.herjavecgroup.com/history-of-cybercrime/
15. www.varonis.com/blog/cybersecurity-statistics/
16. https://undocs.org/A/Res/65/230
17. https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_26/CCCPJ_Res_Dec/CCPCJ-RES-26-4.pdf
18. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html#:~:text=Mandates,capacity%20building%20and%20technical%20assistance.
19. https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html
20. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Draft_decision_5_Aug_2020.pdf
21. https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity
22. https://until.un.org/cybersecurity-challenge
23. https://ideas.unite.un.org/counterdigiterrorism/Page/Home
24. https://undocs.org/S/RES/2341(2017)
25. https://www.bbc.com/news/39655415
26. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
27. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
28. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf
29. https://www.bbc.com/news/technology-38573074
30. https://www.ourcommons.ca/Content/Committee/421/NDDN/Brief/BR9237509/br-external/LitschkoIan-e.pdf

31. https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html
32. https://www.wired.com/story/russian-hackers-attack-ukraine/
33. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/
34. http://www.crime-research.org/library/Cyber-terrorism.htm
35. https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf
36. https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html
37. https://www.pbs.org/newshour/nation/defining-terrorism-consensus
38. https://www.e-ir.info/2019/09/24/terrorism-as-controversy-the-shifting-definition-of-terrorism-in-state-politics/
39. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=195354
40. https://www.state.gov/state-sponsors-of-terrorism/
41. https://www.jstor.org/stable/resrep17466?seq=5#metadata_info_tab_contents
42. https://www.encyclopedia.com/books/encyclopedias-almanacs-transcripts-and-maps/state-sponsored-terrorist
43. https://www.tandfonline.com/doi/abs/10.1080/13537121.2020.1720115?journalCode=fisa20
44. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=191038
45. https://www.amnesty.org/en/what-we-do/death-penalty/
46. https://www.state.gov/reports/country-reports-on-terrorism-2019/iran/
47. https://www.heritage.org/military-strength/assessing-threats-us-vital-interests/iran
48. https://www.cfr.org/backgrounder/iraq-iraqi-ties-terrorist
49. https://www.state.gov/reports/country-reports-on-terrorism-2019/syria/
50. https://www.cfr.org/backgrounder/state-sponsor-syria
51. https://www.un.org/en/ga/sixth/74/int_terrorism.shtml
52. https://www.un.org/sc/ctc/about-us/
53. https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy
54. https://www.un.org/sc/ctc/about-us/
55. https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/
56. https://www.un.org/press/en/2019/sc13754.doc.htm
57. https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/page/4?ctype=Terrorism&cbtype=terrorism#038;cbtype=terrorism
58. https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/?ctype=Iran&cbtype=iran
59. https://www.un.org/press/en/2020/sc14118.doc.htm
60. https://www.securitycouncilreport.org/un_documents_type/security-council-resolutions/?ctype=Syria&cbtype=syria
61. https://usun.usmission.gov/fact-sheet-u-s-introduces-commonsense-resolution-to-extend-arms-embargo-on-worlds-leading-state-sponsor-of-terrorism/

62. https://www.state.gov/state-sponsors-of-terrorism/
63. https://www.e-ir.info/2018/11/14/united-states-foreign-policy-in-the-middle-east-after-the-cold-war/
64. https://www.theatlantic.com/international/archive/2012/05/the-decline-of-state-sponsored-terrorism/257515/
65. https://www.cnn.com/2015/02/19/world/how-isis-makes-money/index.html
66. https://www.state.gov/syria-sanctions/
67. https://www.crisisgroup.org/middle-east-north-africa/eastern-mediterranean/syria/207-averting-isis-resurgence-iraq-and-syria
68. file:///home/chronos/u-c87777d8a64ff93dc5501d9da98bed901889a16a/MyFiles/Downloads/699794.pdf
69. http://arabcenterdc.org/policy_analyses/hamas-plans-a-comeback-to-damascus-us-and-regional-implications/
70. https://afsi.org/2019/03/14/golan-project-israel-exposes-new-hezbollah-cell/
71. https://www.jpost.com/middle-east/hezbollah-presence-in-south-syria-much-larger-than-previously-revealed-648757
72. https://www.jpost.com/arab-israeli-conflict/idf-hezbollah-building-terror-network-on-the-syrian-golan-heights-583272
73. http://www.understandingwar.org/report/hezbollah-syria
74. https://carnegie-mec.org/2019/03/29/power-points-defining-syria-hezbollah-relationship-pub-78730