

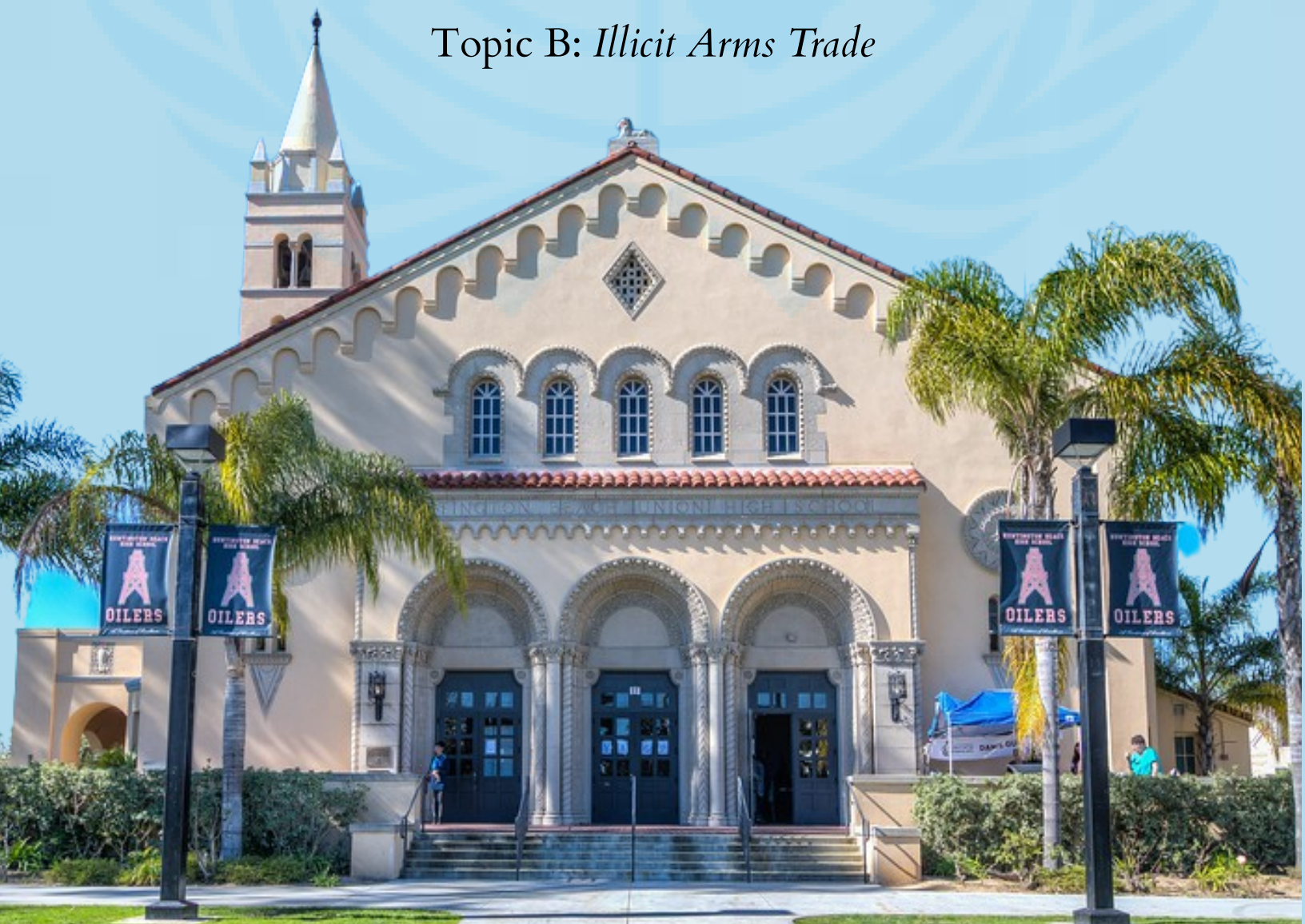
Surf City XIX

Huntington Beach High School

Ad Hoc on Terror

Topic A: *Cyberterrorism*

Topic B: *Illicit Arms Trade*



Welcome Letter

Dear Delegates,

On behalf of the Huntington Beach High School Model United Nations Program, we would like to welcome you to our Surf City XIX 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.

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,



Zach Bernstein
Secretary General



Vivian Bui
Secretary General



Lauren Le
Secretary General



Alison Miu-Martinez
Secretary General

Meet The Dais

Avery Wiley

Hi guys! My name is Avery Wiley and I am currently a senior in my 4th year of MUN here at HBHS. Outside of MUN, I am the captain of field hockey for HBHS and recently finished my last soccer season after playing for over 12 years. After school, I am involved in the National Honors Society and National Society of High School Scholars and I work 4-5 days a week as a hostess and food runner for a small restaurant and brewery called Matter of Craft. I really enjoy surfing and traveling and in my free time I love going on road trips to places like San Onofre, Big Bear, Malibu, and others with my friends. Next year I am planning to double major in forensic science and psychology at a four-year university somewhere on the East Coast and possibly continue my MUN career. I am super excited to meet all you guys in committee and I wish you good luck on your papers! Happy researching and see y'all in February!

Ted Melitas

Hello delegates my name is Ted Melitas and I am a senior at HBHS currently in my 4th year of MUN at the high school. I play varsity soccer at the high school where I have started on varsity for two years as a right wing back and club soccer for CDA Slammers as a center attacking midfielder. Outside of school I work at McDonald's in the Seacliff Center where I work the drive-thru a whopping four hours a week. In my free time I enjoy fishing, practicing soccer, and driving around with my friends. I plan on majoring in environmental engineering next year, where I will hopefully attend a college out of state. However in the meantime I am looking forward to visiting Greece with my friends over the summer. Good luck with your papers, and I will see you all in committee!

Lindsay Alvarez

Hi everyone! My name is Lindsay Alvarez and I will be one of your chairs for this upcoming conference! I am a junior at HBHS and currently in my third year of the Model UN program. When not in school, I play on the HBHS Softball team and am a member of the National Honors Society. I love exploring new places and capturing the beauty of nature with a camera in hand. With my interest in photography, I created the HBHS Photography Club this year and am the club's president. In my free time, you can often find me spending time with my family and friends, making crafts, watching Dodgers games, listening to Taylor Swift, or going to Disneyland. I am really excited to hear your solutions and debate on these ever-growing issues within our world. I cannot wait to see you all in committee!

All Papers are due on **JANUARY 30, 2022** by 11:59 pm to

surfcity.adhocterror@gmail.com

Topic A: Cyberterrorism

Background

Cyberterrorism is the use of the internet or other electronic means to cause harm, infringe on security, or incite violence against a group or government.¹ The practice can cause civil and political unrest and instill great fear into populations and can therefore be used as a weapon by terrorist organizations or individuals. Although the establishment of cyberterrorism is relatively new and the international definition is constantly changing, it is agreed that cyberterrorism must be politically motivated and cause extreme disruption, harm, or fear.² Cyberterrorism is becoming an increasingly pressing issue due to the increased presence and reliance of the international community on the internet and electronic software. As of January 2021, over 4.46 billion people accessed some sort of internet service, giving over 59.5 percent of the entire world population access to the internet.³ The number of internet users is even higher among developed countries with 52.8 percent of people residing in developed nations having access to the internet in 2005 and jumping to 86.7 percent in late 2019.⁴ However, this increasing use of technology—although beneficial for development and technological advancements—puts more people at risk and creates greater secrecy for cyberterrorism and cyber violence-related practices.

Cyberterrorism can be carried out in a plethora of methodologies and by an intricate network of sources, making prosecution and detection extremely difficult. Cyberterrorism is often classified into five main categories for identification purposes: Incursion, Destruction, Disinformation, Denial of Service, and Defacement.⁵ Incursion consists of the intrusion of private information such as classified government files or personal documents in order to gain access to or gain the ability to modify information. Incursion is the most common form of cyberterrorism and gives hackers dangerous information on government defense and security strategies, individual documents and government-issued identification forms, and many other confidential pieces of information. A prevalent example of an incursion attack took place in 2009 when Chinese hackers gained access to the internet server Google's database, giving them personal information such as the names and contacts of Chinese Human Rights Activists.⁶ The series of hacks named Operation Aurora started as a seemingly mundane hunt for personal information and transferred into an attack on US intelligence specifically through US law enforcement agencies by incoherent, rogue Chinese hacking groups. The next classification of cyberterrorism is Destruction which is defined as the purposeful damaging of networks or physical computer software for the purpose of harming an organization and its ability to function. Destruction can cause expensive damage in infrastructural loss and possibly force systems into failure, creating extremely negative effects on the body or agency that relies on the infrastructure to carry out their functions. An example of a destruction hacking incident is the Melissa Virus that gained access into Microsoft and other large corporations' databases, that once opened by an operator, multiplied itself and began destroying software and infrastructure of the network reaping over 80 million dollars in damage.⁷ In addition, the third classification of cyberterrorism is Disinformation. Disinformation occurs when hackers use the internet to create rumors and false information about a corporation, group, or government that causes widespread rejection of the body, having negative effects on the function and structure of the victim. For example, a disinformation attack occurred in France's 2017 election campaign of Emmanuel Macron. Known as the Macron leaks, hackers attempted to spread false information through data leaks of emails and personal conversations in order to discredit Emmanuel Macron and limit his ability to

be elected into the French government.⁸ Then, Denial of Service attacks (DoS attacks) occur when a hacker sends an abnormally large number of requests also referred to as “packets” to an internet service or database that causes the service to incorrectly function, making it unable to process legitimate requests from customers or other accessors. DoS attacks are most common among e-commerce businesses and most frequently attack large online corporations. DoS attacks can be distributed between a plethora of locations and operations classifying the attack as a DDoS or Distributed Denial of Service attack. An example of a DoS attack occurred in Australia in June of 2020 when a state-sponsored organization whose alliance and identity is still frequently debated simultaneously hacked multiple Australian networks and corporations, causing them to be unable to process legitimate requests and fulfill the needs of Australian populations.⁹ This attack caused the Australian Prime Minister to declare a state of cyber emergency in the country and it took days for the government to regain control of the attack concluding with the blame being pointed at Chinese hackers. Finally, Defacement takes place when hackers maliciously attack organizations or government websites and write offensive messages, manipulate the organization of, or make the website unusable. Defacement was once one of the most common types of cyber threats but due to increased awareness of the issue and developments in cybersecurity, the risk and prevalence of defacement crimes have significantly declined. An example of defacement hacking occurred to BitCoin software in 2011 when messages supporting a competitor of BitCoin, called CosbyCoin repetitively showed up on BitCoin’s communication forum.¹⁰

According to IBM Global Security Analysis Lab, about 90 percent of hackers are amateurs and cyberattacks can often be carried out without the extreme malicious intent of cyberterrorism.¹¹ Frequent members involved in cyberterrorism center their attacks around the main goal of causing harm to and weakening a nation, organization, or affiliation group’s support in order to limit their operational capabilities and provide misinformation and distrust in the system. These terrorist organizations also use hacking methodologies to show their legitimacy to other organizations and to their own supporters to establish validity as an organization.¹² Furthermore, attacks on governments and large corporations can instill fear and uncertainty into citizens, causing political unrest and potentially leading to frenzied conflict, ultimately furthering the power and support available to terrorist organizations. Because of the increase in the prevalence of cyber attacks and cyber terrorism and the malicious intent of these hackers, the international community has come together to work towards developing greater cyber security and bettering the technological coalitions that have been created. Among those countries that are most frequently involved in cybercrime and are the largest victims of cyberterrorism, The United States is at the forefront with over 23 percent of all malicious computer activity originating or being aimed at the country.¹³ China and Germany fall second and third in the ranking of malicious computer activity with 9 percent involving China and six percent involving Germany. Cyber attacks and cyber warfare have been deemed the fifth classification of warfare in succession to political, strategic, operational, and tactical warfare proving the immense threat of the practice and further need for cyber security. Additionally, in 2020, reports showed that cyber threats to infrastructure alone posed the fifth greatest threat to international cooperation and individual nation safety and defense, and if cyberterrorism practices increase as studies project, an estimated 10.5 trillion dollars will be lost due to cyber attacks.¹⁴ Action from the international community is needed at the forefront of the battle against cyberterrorism and resolving the ambiguity regarding hackers’ identities and methodologies remains the main concern of involved nations.

United Nations Involvement

Because of the increasing prevalence of cyberterrorism and the need for international unity to provide for greater global cyber security, the United Nations has become gradually more involved in regulations of cyberspace and protections for users of the internet. Under Article 12 of the Universal Declaration of Human Rights which was created to outline the basic protections given to individuals by the international community, the United Nations declares that, “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation”.¹⁵ These protections of privacy work in cooperation with Article 17 of the International Covenant on Civil and Political Rights, drafted by the United Nations Human Rights Office of the High Commissioner which reiterates the Universal Declaration of Human rights and states that it is the individual government’s and international community’s duty to protect and uphold these rights on both a political and civil level.¹⁶ It is because of these outlines of necessary protections of privacy that the United Nations has taken the task of expanding protections of privacy to cyberspace, therefore involving matters of cyber security for the individual user, online corporations, and federal governments.

The United Nations Office of Counter-Terrorism (UNOCT) which deals with terrorism responses and strategies of the UN created a cyber security program to develop a coalition of Member States against specifically infrastructural attacks by terrorist organizations and works to enhance Member State’s capabilities to identify and protect against such attacks.¹⁷ In addition, the Security Council also established its own Counter-Terrorism Committee (CTC) and through Resolution 2341 passed in 2017, connected the CTC with Counter-Terrorism Executive Directorate (CTED), giving them the power to mandate and examine Member State capabilities to increase their protections against cyberterrorism and regulate and monitor their cybersecurity capabilities.¹⁸ The CTED is organized into four pillars outlining the four main goals of the directorate which concern assessment of Member States capabilities and implementations, protections through self-regulation of the private sector, increasing the prevalence of legal restrictions and action regarding infringements on and protections of cyber security, and finally, educating the public on correct cybersecurity strategies to allow them to provide for their own online safety.¹⁹ Security Council Resolution 2129 passed in 2013 also works with the CTED and CTC to strengthen and further develop communications and consultations with the Member States as well as regional and international organizations and the private sector to provide the CTC with the best possible responses to cyberterrorism related issues and matters of cybersecurity, specifically regarding terrorist use of information and communication technologies.²⁰ In coordination with Security Council Resolution 1373 passed in 2001, the CTC has been tasked to identify and notify the Member States of inconsistencies and flaws within their cybersecurity and take note of and share successful implementations with the international community.

Moreover, the General Assembly has also addressed matters of cyberterrorism, focusing mainly on safety provisions and cohesive condemnation for the international community. For example, in the 73rd session of the General Assembly, the UN addressed the ransom ware WannaCry that attacked over 43,000 devices, the GA worked in cohesion with the 1st DISEC’s A/Res/74/2019 and A/Res/73/2018 to condemn international use of ransomware and create a criminal prosecution based approach to the cyberterrorism practice.²¹ Through this approach UN bodies were able to hold attackers guilty, develop more identification methodologies and possibly take matters of cyberterrorism to the International Criminal Court if a large, violent attack was determined to disrupt peace.

Case Study: Titan Rain

Titan Rain was a series of cyber attacks and operations that exposed various US and UK government agencies. The 2003 string of attacks originated from Guangdong, China, and the perpetrators were assumed to be members of the People's Liberation Army Unit 61398. The hackers targeted the Defense Intelligence Agency in the US and the Ministry of Defense in the UK, waging cyber warfare that lasted just over three years, notably shutting down half of the computer systems in the UK House of Commons in 2006.²² Moreover, in the US, hackers gained access and passwords to highly sensitive information found on the US defense contractors' networks. Companies including NASA, Redstone Arsenal, Sandia National Laboratories, and Lockheed Martin were all compromised through the series of attacks. This meant that the Titan Rain hackers had access to classified US defense and attack information, which could have had devastating lasting effects on the nation's security. For example, Lockheed Martin provides the US with almost all of its missile defense systems, fighter jets, missiles, as well as other military elements of vast importance. Since the hackers had stolen the military's passwords, they had access to complete receipts of the US military's total purchases, providing the Chinese government with crucial information regarding our countries security.²³ Additionally, Sandia National laboratories control the reliability, and safe containment of nuclear weapons as well as providing the nation with nonproliferation and nuclear defense technologies. Following these attacks, the Titan Rain hackers gained access to US nuclear processes, allowing them to mimic defense and testing procedures.²⁴ Redstone Arsenal, dating back to World War II, is the United States' military center for missile and rocket programs, in addition to being the nation's largest provider of chemical weapons. Similarly to the Lockheed Martin attacks, a similar outcome to this series of cyber raids allowed for the increased intelligence on US arsenals, possessed by the Chinese government.²⁵ Finally, NASA or the National Aeronautics and Space Administration oversees all government-sponsored space exploration and travel initiatives. Furthermore, the presence of NASA satellites in space allows for momentous scientific discovery regarding Earth, as well as planets, solar systems, and galaxies beyond our own. Although no encrypted data was stolen when the organization was attacked, employee identification and passwords were uncovered, however thankfully, no repercussions to these actions have been reported.²⁶ The state of the nation's safety lies with companies and organizations, such as the aforementioned, and the idea that such power was placed in the hands of a foreign nation rattled the American population.

Following the 2003-2004 attacks, the US and UK governments held the Chinese government responsible for the orchestration of the events. Refuting all claims of government affiliation with the hackers, the Chinese government suggested an alternative theory. The Chinese government theorized that a group of independent hackers used Chinese computers and websites in order to launch a cyberterrorism attack against the United States. Although the Chinese statement held some validity, seeing as the nation had struggled with internal internet security before, the case was still stacked against the nation. Seeing as the level of intricacy and organization the hackers would have needed to have completely launched and sustained a cyber attack against the US and UK was on par with the aforementioned countries military standards, it raised suspicion regarding the honesty of the Chinese government. Moreover, the sheer size of the attack did not line up with the independent party story told. Backing up the suspicions, Adam Paller, a research director at SANS institute which is the front running independent organization relating to cybersecurity training, research, and certifications, claimed that the 2004 attacks were too precise to be random hackers and that the discipline required excluded all parties except a highly trained military. It is circumstances such as these, where the international community


advocates for one theory, while an individual preaches another, that have prevented cyberterrorism from being fully defined and prosecuted. Due to secrecy between nations, as well as political orientations pitting nations against each other, the origin of a cyberattack is almost impossible to be directly pinned. Moreover, international law prevents transnational prosecution in some circumstances, meaning if the international community comes to a complete consensus, there is still nothing that can be done to stop acts of cyberterrorism from occurring or prosecute those responsible.²⁷

Titan Rain was the catalyst for the extreme mistrust in China regarding operations in cyberspace, especially in the United States, but extending to other nations as well. Additionally, the political fallout from the attacks was intense as the FBI began relentlessly investigating the situation, hiring public and private parties, to spy on and research the source of the attack as well as any related sources. Although independent parties were helpful to some extent, internal conflicts began to arise because of actions that were taken. The case of Shawn Carpenter captivates the embodiment of the predicament. Since the FBI does not have the mandatory skills nor technology to track down foreign hackers, independent “vigilantes” take it upon themselves to solve the situation. Such is the situation of Carpenter, while researching and spying on secret servers, chat rooms, and networks, he would relay his information to unofficial army contacts he had created while working for Sandia National Laboratories. Although federal law prohibits the relaying of information between army intelligence and civilians, a loophole allowed for Carpenter to work under the FBI as a confidential informant. Although helpful, his actions violated US law, stating that Americans are not allowed to hack into the computers of foreign nations. Stripped of his government clearance, as well as fired from his job, an outraged Carpenter filed a lawsuit against Sandia for wrongful termination. Even though Carpenter was fired and his work was denounced, the complexity of the situation remained. While the FBI was conducting an investigation into Carpenter’s accounts, they came across a homemade tracking code that he had made himself, giving the FBI the ability to stalk the Titan Rain hackers, which ultimately led to the de-escalation of the crisis.²⁸

Following the events of the Titan Rain attacks, the public sector became aware that in many cases public and private networks can go unprotected by government agencies, and in many ways, the last line of defense against cyberattacks can be uber hackers like Carpenter. Moreover, companies with well-trained IT managers and CIO’s can do their best to practice and teach safe and reliable internet techniques. Ultimately, however, as was scarily uncovered during the events of Titan Rain, the cyber world can go unprotected.²⁹

Questions to Consider

1. What actions can governments take to detect cyber attacks and what, if any, prosecutions should be placed upon those found guilty of a cyber attack?
2. What measures can governments take to protect national users and private corporations from cyberterrorism?
3. What does your country define as cyberterrorism? And what measures can be taken to provide a comprehensive definition to resolve inconsistencies throughout the international community?
4. Has your country ever been a victim of a cyber attack? If so, what measures were taken to combat the attack? If not, what policies or protections have been successful to deter the threat of cyberattacks in your country?

- 
- A large, faint, light-gray watermark is visible in the background of the page. It consists of a globe in the upper half and a stylized building with a pointed roof and several windows in the lower half.
5. Does your country believe that monitoring initiatives and methodologies should be implemented to protect the cybersphere? Why or why not?
 6. What role can private companies have in preventing cyberterrorism? Often owning popular Internet search engines or social media platforms, to what extent can these private companies use their platforms to educate the public on past terrorist attacks or strategies to protect their cybersecurity?

Endnotes

1. <https://blog.logsign.com/what-are-cyberterrorism-and-cyberwarfare/>
2. <http://www.computerworld.com/article/2492864/cybercrime-hacking/un--more-international-cooperation-needed-to-fight-cyberterrorism.html>
3. <https://www.statista.com/statistics/617136/digital-population-worldwide/>
4. <https://www.statista.com/statistics/209096/share-of-internet-users-in-the-total-world-population-since-2006/>
5. <https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf>
6. <https://www.express.co.uk/news/world/1373272/google-gmail-youtube-down-hack-cyber-attack-china-operation-aurora-security-breach-spt>
7. <https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519>
8. <https://www.enisa.europa.eu/publications/info-notes/disinformation-operations-in-cyber-space>
9. <https://theconversation.com/australia-is-under-sustained-cyber-attack-warns-the-government-whats-going-on-and-what-should-businesses-do-141119>
10. <http://alphavilleherald.com/2011/09/cosbycoin-forum-hack-pops-bitcoin-forum-bubble.html>
11. <https://www.ibm.com/security/security-expert-labs>
12. <https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154#:~:text=There%20are%20five%20main%20types,others%20and%20have%20different%20objectives>
13. <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>
14. <https://www.albawaba.com/business/10-biggest-cyber-attacks-history>
15. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
16. <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>
17. <https://www.un.org/counterterrorism/>
18. [https://undocs.org/S/RES/2341\(2017\)](https://undocs.org/S/RES/2341(2017))
19. <https://www.ohchr.org/Documents/Issues/RuleOfLaw/PCVE/CTED.pdf>
20. [https://undocs.org/en/S/RES/2129\(2013\)](https://undocs.org/en/S/RES/2129(2013))
21. <https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf>
22. <https://tophackers.wordpress.com/8-titan-rain/>
23. <https://www.lockheedmartinjobs.com/getting-to-know#:~:text=We%20develop%20high%2Dperformance%20air,systems%20and%20energy%20storage%20solutions>
24. <https://www.sandia.gov/>
25. <https://home.army.mil/redstone/index.php>
26. <https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-nasa-58.html>
27. <https://cyware.com/news/remembering-operation-titan-rain-c54ad3e4>
28. https://courses.cs.washington.edu/courses/csep590/05au/readings/titan_rain.htm
29. <https://www.computerworld.com/article/2559195/guard-against-titan-rain-hackers.htm>

Topic B: Illicit Arms Trade

Background

The illicit arms trade can be defined as the illegal purchase, selling, and organized trade of firearms, relevant components and parts, as well as ammunition across or within country borders. These transactions include grey market illicit sales, in which a government or organization exploits a loophole to proceed with their activities, this also includes lost, misplaced, or souvenir arms (or other like replicas that can be altered into an evenly performing gun); as well as black market illegal transactions that take place without government oversight or control, illegally. Although occurring mainly in areas of economic or violent turmoil, the illicit arms trade is an issue that affects nations globally. Moreover, the process, also frequently referred to as gun-running and arms trafficking is estimated to bring in over 1 billion US dollars annually to various sources, as well as account for over 600 million unregistered illegal firearms in UN member nations, according to a 2015 study.¹ The small arms and light weapons (SALW) is one of the most important aspects of the illicit trade as it directly relates to other areas of illegality, seeing as they provide for a majority of income and use for terrorist and other independent groups. Small arms are classified as weaponry that is made and intended to be used by only one person, including but not limited to, sniper and assault rifles, submachine guns, as well as pistols. On the other hand, light weapons are generally larger, more expensive, and require more effort to use, consisting of, recoilless rifles, mounted machine guns, and various explosive devices including anti-air crafts weapons as well as grenade launchers.²

The demand for illicit arms or weaponry, in general, is one of the main contributors to the prevalence of the issue. The aforementioned demand stems from various sources including areas with high levels of civil unrest, crime, or violence. Whether the crime is organized or local, both lead to an increase of illicit arms and its trade within the area. An increase in civil unrest creates a weaker government, allowing the area for illicit trade to increase.³ The next contributor to illicit arm demand is the presence of large armed conflict within a region in which guns would be desirable for a multitude of reasons. First, many of these conflicts are fought with SALW between extremist independent groups, as well as underdeveloped governments making the presence of illicit arms inevitable. However if fought between two large nations, the increased demand would still be prevalent as illicit arms may be cheaper and more readily available during a large armed conflict. Moreover, through violent unrest, citizens or parties not involved in the conflict may inquire firearms for protection, and if they do not have the resources or ability to get the gun properly licensed, they will turn to illicit means.⁴ Additionally, mistrust within the security sector can lead to an increase in illicit arms activities, specifically when security forces seem to be or are unable to protect citizens. This would cause citizens to take their security personally, purchasing their own firearms. Weak security forces, as well as an increase in terrorist or other extremist presences, can lead to humanitarian violations and make citizens feel that they are unsafe, therefore leading to increased arms purchases.⁵ Finally, low civilian representation in government decision-making leads to an increased demand for illicit arms. In many cases, low representation leads to rebellion which often becomes violent. To arm themselves against what they believe to be an unfit government, citizens in places with low political representation will often go around the government restrictions and laws surrounding the selling and buying of firearms, thus obtaining the guns elsewhere.⁶

There are three main sources of firearms that fuel the illicit trade. Illicit manufacturing, which is the new creation of guns, follows blueprints and designs of previously existing weapons. Illicit manufacturing was exemplified in a 2011-2012 investigative study that revealed that in Sao Paulo alone over 14,400 sub-machine guns were seized from illicit facilities. Moreover, it was reported that over 48% of these firearms were homemade, proving the expansion of illicit manufacturing practices. In addition, a 2017 report disclosed that two homemade gun factories were uncovered in Australia and the Philippines. The factories were discovered to be creating .22 rifle replicas and .22 caliber pen guns, respectively.⁷ The next main source of firearms provided for illicit trafficking is theft or diversion. In this process, guns are stolen from legal tenders, government stockpiles, or acquisition from other legal arm transfers. One example of this could be leakages and theft from a manufacturer. For instance, an employee could steal a gun from the production facility and sell it on the black market, or sell malfunctioning parts or guns as a whole, to be fixed and utilized. Another example would be following the end of the Cold War, where the surplus of weapons possessed by NATO and Warsaw Pact nations were sold at bargain prices on the global market. These firearms and ammunition trickled down into the hands of terrorist organizations, extremist parties, and illicit arms dealers.⁸ The final source of illicit arms practices is conversion, which is the recycling or altering of weaponry to serve illicit purposes.⁹ For example, the United Nations Development Program's SAWL project in the Balkans reported an influx in the conversion of replicas and blank pistols into fully functioning weaponry. Another example of conversion methodologies takes advantage of the replica firearm market. The market for famous weaponry, movie props, as well as other important or well-known replicas requires guns to be deactivated. However, through a skilled and precise process, these weapons can be restored to full use, to be sold or utilized in a very profitable business exchange. In various Irish and English cities such as Dublin, Glasgow, and Manchester, there was an increase in shooting and armed robberies, sporting reactivated Mac-10 submachine guns. Luckily, the police were able to trace the weapons to a small workshop where over 40 deactivated Mac-10's were seized, costing only 100 dollars each, however when flipped, could bring in 10 times that.¹⁰

In continuation, there are three main types of large-scale delivery techniques utilized by buyers and sellers that often go undetected by government arms regulations. First, concealment is most commonly used in underdeveloped, underenforced regions, where the theft of arms will most likely go uncovered and untracked. The stolen arms are simply covertly carried across borders during secure hidden transactions. The next practice, point of departure diversion, takes advantage of fraudulent or altered end-user identification or certification. Through the point of departure diversion process, SALWs are never transferred or shipped to the assumed, correct end user. Finally, post-delivery onward diversion utilizes fraudulent or ostensibly altered verifications to hide and complete transactions.¹¹ The goals of illicit arms dealers are based on private gain and are not correlated with state government efforts, however many times smugglers work together to form more complex operations regarding large-scale deliveries. For example, existing demand, which is the process in which dealers of illicit arms may join forces with other dealers to kill members of rival operations and other legal tenders of arms. Moreover, Existing supply where private stockpile holders may defend their arms. As well as expertise in which private organizations hire trained figures to aid purchasers of weaponry in its safe use and regulation.¹²

Following the resolution of the Cold War and the destruction of the Soviet bloc, there was a momentous increase in SALW weaponry specifically within Africa. This made Africa the epicenter for illicit arms trade and armed conflict. In the following years, many African regions saw an influx in arms trade as well as illegal weapons-related activities. In many areas, it was reported that one could buy a soviet AK-47 for six dollars and that in Somalia's capital city of

Mogadishu, the number of firearms present in the city was almost equal to the 1.3 million people living in the city. In addition, a US government estimate saw that 7-8 million deaths have occurred within 22 African countries due to SALW armed conflict. The weapons that have been brought into the African continent and many others around the globe by the Soviet Era have spawned a culture of gun violence, that will continue to grow if fueled by the illicit arms trade.¹³

United Nations Involvement

In the 1998 A/RES/53/111, the UN Ad Hoc Committee on the Elaboration of a Convention against Transnational Organized Crime was created to prevent the illicit manufacturing and trade of firearms globally.¹⁴ In 2000, this Ad Hoc Committee established the UN Convention against Transnational Organized Crime in A/RES/55/25.¹⁵ Meeting for 13 sessions between 1999 and 2004, the committee drafted the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition (Firearms Protocol), which was ultimately adopted in A/RES/55/255. Serving as a document to legally bind nations to mitigate the illicit arms trade, the Firearms Protocol aims to implement data collection measures, record firearms, and regulate imports and exports to prevent arms from entering illegal pathways.¹⁶

Adopted in 2001, the UN Programme of Action to Prevent, Combat, and Eradicate the Illicit Trade in Small Arms and Light Weapons (PoA) works to combat the illicit trafficking and manufacturing of small arms worldwide.¹⁷ Although the PoA deals solely with small arms and light weapons, these arms are the most common illegally trafficked items, accounting for a \$1 billion black market. The PoA serves as a global politically binding treaty, urging nations to improve their management of weapons, regulation laws for arms trade, and its control over arms imports and exports. Alongside the PoA, the 2005 International Tracing Instrument (ITI) aims to reduce weapons trafficking through global cooperation of record-keeping, marking, and tracing.¹⁸

The Arms Trade Treaty (ATT) is one of the primary UN efforts to reduce illicit arms trafficking worldwide, focusing on creating standards for the trading and transferring of weapons internationally.¹⁹ Adopted in 2014, the ATT has 141 signatories, with 110 of those nations having ratified the treaty.²⁰ The ATT calls for its State Parties to create a national control list to regulate the number of conventional arms being exported and imported in their nation.²¹ Under the ATT, arms cannot be exported if thought to be used in civilian attacks or genocide, breach the 1949 Geneva Convention, or violate arms embargoes or international treaties. Although the ATT has made strides to combat the global illicit arms trade, 54 nations where it is most prevalent, including Saudi Arabia, Russia, and Sudan, have not signed the treaty. The U.S., accounting for 35% of arms sales globally, also announced in 2019 that it will remove its signature from the ATT, claiming that the treaty's regulation of conventional arms violated their right to bear arms.²²

The United Nations Trust Facility Supporting Cooperation on Arms Regulation (UNSCAR) also encourages nations to regulate conventional arms through a multi-donor trust fund of NGOs, UN partners, and other international organizations.²³ Since its creation in 2013, UNSCAR has given \$9 million in funding to 64 different arms regulation projects worldwide, including the creation of databases, implementation tools, and managing arms stockpiles.

The need to mitigate the illicit arms trade has also been shown in the 2030 Agenda for Sustainable Development Goals (SDGs).²⁴ More specifically, SDG 16.4 calls upon nations to record, trace, and destroy arms while also ensuring that these efforts abide by existing international regulations. To fulfill these aims, the United Nations Office for Disarmament Affairs (UNODA) works alongside nations to implement accurate data collection for its arms

trade. Currently, the UNODA works in regions in Latin America, Asia and the Pacific, the Caribbean, and Africa to combat the illicit arms trade and uses the ATT to guide its efforts.²⁵

To reduce the illicit arms trade, the UN has placed embargoes on nations including Libya, South Sudan, the Central African Republic, and Somalia.²⁶ Created in S/RES/1874 in 2009, a UN arms embargo was also placed on North Korea, prohibiting all imports and exports of weapons in alignment with the UN Register of Conventional Weapons to or from North Korea.²⁷

Several resolutions to combat the global illicit arms trade have also been passed by the UN. For example, S/RES/2220 calls upon nations to monitor arms trade regulations, maintain the existing UN embargoes, and collaborate globally to uncover potential arms traffickers or illicit trading routes.²⁸ S/RES/2220 also urges nations to work with the Counter-Terrorism Committee Executive Directorate (CTED) to reduce the number of illicitly trafficked arms specifically sent to terrorist organizations, who use the weapons to violate the peace and security of society.

Case Study: Illicit Arms and the Yemen Civil War

Initially beginning in 2014, the civil war in Yemen continues to persist in the present day, with the conflict largely fueled by the illicit arms trade. Growing tensions in Yemen were initially sparked in 2011, resulting in the shift of power from Yemen's long-time president, Ali Abdullah Saleh, to his then vice-president Rabbu Mansour Hadi.²⁹ After Hadi gained power, however, Yemen's capital of Sana'a was overtaken by Houthi rebels in 2014, serving as a catalyst for the Yemen Civil War to begin.³⁰ Although the UN has attempted to foster peace talks among the conflicting groups, the civil war began with two sides: Saleh backed by the Houthi rebel group and Hadi backed by Saudi Arabia troops. Currently totaling 100,000 deaths from the ongoing conflict and weapons trafficking vastly contributing to the 15 million firearms already in its borders, the UN has labeled Yemen as "the largest humanitarian crisis in the world."³¹

Yemen continues to be a region that experiences a high prevalence of weapons and, as a result, the illicit arms trade increasingly grows as well. When the civil war initially sparked, Yemen was already ranked second in the most heavily armed nations worldwide, accounting for a 54% gun prevalence among its citizens in 2014.³² As the war has waged on, however, the thousands of weapons from the illicit arms trade in Yemen has ultimately increased the number of arms by 300%.³³ More specifically, these arms often originate in Western or other developed nations including the United States and China, which then distribute the weapons mainly to Iran and Saudi Arabia. However, researchers such as the Control Arms Coalition's Anna MacDonald have noted that Iran and Saudi Arabia then illicitly smuggle the weapons to Yemen in a third-party trade, using the conflict as a proxy war to gain dominance within the Middle East.³⁴ In addition, Iran supports the Houthis through the illicit arms trade in hopes of creating a primarily Shia Muslim state, while Saudi Arabia is also fueling Hadi's supporters to implement a mainly Sunni Muslim state. As the civil war has progressed, however, the illicit arms trade has become increasingly prevalent on both sides of the war: the Houthis and Hadi's supporters.

To fuel the ongoing civil war, the Houthis rely on the illicit arms trade to provide their forces with new weapons for battle. The United Nations has continuously shown its support for President Hadi, believing that the Houthi rebels violate the peace and security of Yemen. Most notably, denoting that the Houthis use imported weapons to fuel the Yemen Civil War and cause violence, the Security Council adopted S/RES/2216 in 2015. In this resolution, an embargo was placed on Yemen to prevent the supply of items including arms, ammunition, and other weapons that serve to support the Houthis.³⁵ Although this arms embargo has been enacted, Iran has continued to illicitly trade weapons to the Houthis in Yemen. The trafficking of weapons to the

Houthis in violation of the embargo occurs in two main methods: shipping in waterways with dhows or overland routes through other nations. First, since the outbreak of the war, the Global Initiative against Transnational Organized Crime has stated that 13 dhows, or private vessels, carrying 400 illicit weapons have been caught.³⁶ Of these, a 2018 shipment of 178 automatic rifles and 48 grenade launchers were seized in the Gulf of Aden.³⁷ Upon review by the Panel of Experts on Yemen, they determined the arms were intended for the Houthis to fuel the ongoing civil war. In addition, the Panel noted that the manufacturer of the automatic rifles in the shipment could be traced back to China and the grenade launchers had vast similarities to Iran's manufactured RPG-7 arms. Although these illicit arms shipments to Yemen included weapons from China, the Panel confirmed the weapons were initially given legally to Iran from China, but were then illegally trafficked by Iran to the Houthis through a violation of the UN arms embargo. In addition to the use of waterways, overland routes are also used by Iran to illicitly supply arms to the Houthis. More specifically, Iran illicitly trades small arms, short-range missiles, and other weapons to Yemen through the country of Oman.³⁸ In 2016, trucks bearing Oman license plates traveling to the Houthis were intercepted, illegally carrying arms and other weapons that breach Yemen's arms embargo. Despite these efforts, Oman's authorities continue to claim that they are neutral in the Yemen Civil War and decline the prevalence of illicit arms trade involving the nation's borders. Illegally smuggled to the Houthis through the 288-km Yemen-Oman border, these arms ultimately contribute to thousands of civilian deaths each year. For example, Iran's illegally traded ballistic missiles to the Houthis were used in an attack on a religious school in Yemen earlier in 2021, resulting in the death of 29 innocent individuals.³⁹ Therefore, Iran poses not only as a threat to the previous 2014 UN arms embargo on the Houthis, but its actions have catalyzed the growth of the illicit arms trade and the Houthi's violence in the Yemen Civil War.

Although Hadi and his supporters in Yemen's government do not have an embargo, they continue to fuel the civil war in the illicit arms trade through a violation of the Arms Trade Treaty. Many Western states export billions worth of weapons to Saudi Arabia; for example, within a year of the war's outbreak, the United States supplied \$5.9 billion worth of weapons, the United Kingdom supplied \$4 billion, and France supplied \$18 billion. Even though the transfer of weapons between Western nations and Saudi Arabia is considered a legal arms deal, thousands of these arms are then illicitly traded to pro-Hadi forces because they have been denoted as causing "war crimes". According to the Yemen Data Project, of the weapons from Saudi Arabia, one-third have targeted non-military areas—hospitals, schools, or marketplaces. As a result, the Western powers that initially supplied the weapons to Saudi Arabia have been noted by the UN Group of Eminent Experts as violating humanitarian law, determining their transfers of weapons as illicit.⁴⁰ This poses a large violation to the 2014 ATT, which France and the UK have both ratified, stating that arms cannot be transferred if thought to be engaged in "attacks directed against civilian objects or civilians."⁴¹ In light of the Yemen Civil War humanitarian crisis, the United States has taken action to reduce their transfer of weapons to Saudi Arabia.⁴² Although the U.S. served as one of Saudi Arabia's main arms suppliers during President Trump's 2015 to 2019 term, accounting for \$31.4 billion worth of arms exports, President Biden stated that the U.S. would temporarily freeze its arms sales to the nation earlier in 2021.⁴³ However, other nations that have announced similar arms suspensions to Saudi Arabia have not abided by their aims. For example, the UK halted its arms sales to Saudi Arabia in 2019; however, it was ultimately resumed in one year after it deemed the arms trade did not violate humanitarian law.⁴⁴

Despite efforts from the United Nations and other countries, the illicit arms trade continues to pose a vast threat to the Yemen Civil War. On the Houthi side of the conflict, Iran uses both waterways in the Gulf of Aden and overland routes through Oman to illegally smuggle these weapons in violation of the Houthis' UN arms embargo. For Hadi and his supporters,

however, the third-party illicit arms trade between Western countries to Saudi Arabia to Yemen has gained international recognition as breaching humanitarian law and the ATT. Therefore, nations must work to halt the illicit arms trade's prevalence in Yemen as it is vital to help end the civil war and prevent millions of civilians from being harmed in its aftermath.

Questions to Consider

1. How is your country affected by the illicit arms trade within its borders? And what actions, if any, has your country taken in regards to regulating the expansion of the illicit arms trade into its borders?
2. What previous United Nations actions has your country supported regarding the mitigation of illicit arms activities?
3. What types of small arms are most actively trafficked in your country and the areas surrounding your country and why?
4. Has your country been involved in previous agreements regarding the illicit arms trade? And if so, with what countries or organizations and for what reasons were the agreements created?
5. What large-scale delivery technique is the most prevalent within your country regarding the illicit arms trade and has any governmental actions been taken to combat this methodology?
6. How can you ensure nations who play a prevalent role in the illicit arms trade regulate their weapons exports and imports? Have there been weapon-tracing methods that have shown success in either your country or other nations in the past?
7. What regulations, if any, should be placed on the purchase and trade of ammunition? What international regulations have been placed on ammunition specifically?

Endnotes

1. <https://www.interpol.int/en/Crimes/Firearms-trafficking>
2. <https://www.un.org/disarmament/convarms/salw/>
3. https://www.unodc.org/documents/data-and-analysis/Firearms/2020_REPORT_Global_Study_on_Firearms_Trafficking_2020_web.pdf
4. <https://www.unodc.org/unodc/en/firearms-protocol/firearms-study.html>
5. <https://everytownresearch.org/issue/gun-trafficking/>
6. <https://www.amacad.org/news/arms-trafficking-its-past-present-and-future>
7. https://www.unodc.org/documents/e4j/Module_04_-_The_Illicit_Market_in_Firearms_FINAL.pdf
8. https://www.unodc.org/documents/e4j/Module_04_-_The_Illicit_Market_in_Firearms_FINAL.pdf
9. <https://illicittrade.org/illegal-arms-trafficking>
10. https://www.unodc.org/documents/e4j/Module_04_-_The_Illicit_Market_in_Firearms_FINAL.pdf
11. <https://www.unodc.org/e4j/en/firearms/module-4/key-issues/supply--demand-and-criminal-motivations.html>
12. <https://www.unodc.org/e4j/en/organized-crime/module-3/key-issues/firearms-trafficking.html>
13. <https://www.un.org/africarenewal/magazine/december-2011/small-arms-africa>
14. https://treaties.un.org/doc/source/docs/A_RES_55_255-E.pdf
15. <https://legal.un.org/avl/ha/unctoc/unctoc.html>
16. <https://www.unodc.org/unodc/en/firearms-protocol/the-firearms-protocol.html>
17. <https://unrepcd.org/conventional-weapons/poa/>
18. <http://www.weaponslaw.org/instruments/2005-international-tracing-instrument>
19. https://www.armscontrol.org/factsheets/arms_trade_treaty
20. <https://www.un.org/disarmament/conventional-arms/>
21. <https://thearmstradetreaty.org/reporting.html>
22. <https://www.armscontrol.org/act/2019-05/news/us-quit-arms-trade-treaty>
23. <https://front.un-arm.org/wp-content/uploads/2018/07/UNSCAR-Fact-Sheet-July2018.pdf>
24. https://www.un.org/disarmament/wp-content/uploads/2015/02/UNODA-SDG-Primer_v2.pdf
25. <https://www.un.org/disarmament/convarms/att/#collapse4>
26. <https://www.swp-berlin.org/10.18449/2020C23/>
27. https://www.sipri.org/databases/embargoes/un_arms_embargoes/north_korea
28. [https://undocs.org/S/Res/2220\(2015\)](https://undocs.org/S/Res/2220(2015))
29. <https://www.britannica.com/place/Yemen/War-of-secession-and-political-unrest>
30. <https://www.cfr.org/global-conflict-tracker/conflict/war-yemen>
31. <https://www.unicef.org/emergencies/yemen-crisis#:~:text=Yemen%20is%20the%20largest%20humanitarian%20crisis%20in%20the%20world%2C%20with,hell%20for%20the%20country's%20children.>
32. <https://jamestown.org/program/yemen-dangerous-regional-arms-bazaar/>
33. <https://insidearabia.com/weapons-trafficking-fuels-conflicts-in-yemen-and-africa/>
34. <https://www.reuters.com/article/us-yemen-security-arms/arms-sales-to-saudi-illicit-due-to-civilian-deaths-in-yemen-campaigners-idUSKCN10X1MM>
35. [https://www.undocs.org/S/RES/2216%20\(2015\)](https://www.undocs.org/S/RES/2216%20(2015))
36. <https://www.reuters.com/world/iranian-supplied-arms-smuggled-yemen-into-somalia-study-says-2021-11-10/>

37. <https://undocs.org/en/S/2020/326>
38. <https://www.fdd.org/analysis/2018/03/12/oman-needs-to-prevent-iranian-weapons-shipments-to-houthis/>
39. <https://www.reuters.com/world/middle-east/official-houthi-missile-attack-kills-injures-29-civilians-yemens-marib-minister-2021-11-01/>
40. <https://www.hrw.org/world-report/2020/country-chapters/yemen#>
41. https://thearmstradetreaty.org/hyper-images/file/ATT_English/ATT_English.pdf?templateId=137253
42. [https://thearmstradetreaty.org/hyper-images/file/List%20of%20ATT%20States%20Parties%20\(alphabetical%20order\)\(07%20August%202020\)/List%20of%20ATT%20States%20Parties%20\(alphabetical%20order\)\(07%20August%202020\).pdf](https://thearmstradetreaty.org/hyper-images/file/List%20of%20ATT%20States%20Parties%20(alphabetical%20order)(07%20August%202020)/List%20of%20ATT%20States%20Parties%20(alphabetical%20order)(07%20August%202020).pdf)
43. <https://reliefweb.int/report/yemen/g20-arms-exports-saudi-arabia-worth-three-times-aid-yemen-2015-oxfam>
44. <https://controlarms.org/blog/halt-arms-sales-for-use-in-yemen>