North Atlantic Treaty Organization
Dear Delegates,

My name is Allan Lee and I am honoured to serve as your director of the North Atlantic Treaty Organization (NATO). As a grade 11 student at St. George’s, I am very excited to participate in VMUN 2018—my fourth VMUN since grade 8. This is my first time directing and I am more than excited to be doing so. I have participated in MUN since grade 8 in local conferences and even some international conferences. Throughout all of my experiences in MUN, I have improved my grasp on global issues, engaged with other views and perspectives, diversified my set of knowledge, and argued my points to the best of my ability. Other than MUN, I also debate, play music, and volunteer. Along with me are two incredibly competent staff members that will make this weekend possible — Inaya Ali as your Chair and Roberto Xavier as your Assistant Director (AD). Inaya is currently a grade 11 student at Port Moody Secondary who enjoys playing basketball and spends time volunteering. Roberto, who is from Brazil, is a grade 12 student at St. George’s who enjoys playing rugby, watching movies. Inaya, Roberto, and I hope to bring the best experience to all delegates in VMUN 2018.

The two topics I have chosen — Cyber Terrorism and Security in Afghanistan — are both pertinent issues with catastrophic consequences if not dealt with properly. Both issues are nuanced and complex. As NATO, it is of utmost importance that these issues are treated delicately with respect to those affected. Thus, it is important that every delegate contribute and discuss a variety of ideas to create the most successful resolution possible to counter those who actively cause harm to innocent lives and protect our allies.

I wish everyone the best of luck in preparation for this conference. Please do not hesitate to contact myself or the staff members. We are incredibly excited for VMUN 2018 and we wish everyone the best experience possible.

Sincerely,

Allan Lee
NATO Director

Ken Hong
Secretary-General

Callum Shepard
Chief of Staff

Jerry Jiao
Director-General

Andrew Wei
Director of Logistics

Jadine Ngan
USG General Assemblies

Eric Zhang
USG Specialized Agencies

Dillon Ramlochun
USG Conference

Angelina Zhang
USG Delegate Affairs

Jerry Xu
USG Delegate Affairs

Alan Chen
USG Finance

Meghna Lohia
USG IT
Position Paper Policy

What is a Position Paper?
A position paper is a brief overview of a country's stance on the topics being discussed by a particular committee. Though there is no specific format the position paper must follow, it should include a description of your positions your country holds on the issues on the agenda, relevant actions that your country has taken, and potential solutions that your country would support.

At Vancouver Model United Nations, delegates should write a position paper for each of the committee's topics. Each position paper should not exceed one page, and should all be combined into a single document per delegate.

Formatting
Position papers should:
— Include the name of the delegate, his/her country, and the committee
— Be in a standard font (e.g. Times New Roman) with a 12-point font size and 1-inch document margins
— Not include illustrations, diagrams, decorations, national symbols, watermarks, or page borders
— Include citations and a bibliography, in any format, giving due credit to the sources used in research (not included in the 1-page limit)

Due Dates and Submission Procedure
Position papers for this committee are mandatory. The submission deadline is January 7th, 2018.

Once your position paper is complete, please save the file as your last name, your first name and send it as an attachment in an email, to your committee's email address, with the subject heading as your last name, your first name — Position Paper. Please do not add any other attachments to the email or write anything else in the body.

Both your position papers should be combined into a single PDF or Word document file; position papers submitted in another format will not be accepted.

The email address for this committee is nato@vmun.com.
Countering Cybercrime

Overview ................................................................................................................................................. 6
Timeline ................................................................................................................................................... 6
Historical Analysis ........................................................................................................................................ 8
Past UN and International Involvement ............................................................................................... 10
  International Criminal Police Organization (INTERPOL) ................................................................. 10
  United Nations (UN) .......................................................................................................................... 10
  Private Entities ....................................................................................................................................... 10
  Case Study: The Prosecution of Kevin Mitnick ................................................................................. 11
Current Situation .................................................................................................................................. 11
  Types of Cyber Attacks ....................................................................................................................... 11
  Difficulties in Fighting Cyberterrorism ............................................................................................. 12
  State-sponsored Attacks ...................................................................................................................... 13
  Criminal Organizations ...................................................................................................................... 13
  Hacktivism .......................................................................................................................................... 13
Possible Solutions ................................................................................................................................ 14
  Cyber Weapons ................................................................................................................................... 14
  Increased Surveillance/Restricted Online Access .............................................................................. 14
  Increased NATO Presence and Support ............................................................................................. 14
  Cooperation with Private Entities ......................................................................................................... 15
Bloc Positions ........................................................................................................................................ 15
  Baltic States ......................................................................................................................................... 15
  European States .................................................................................................................................. 15
  Major Powers ....................................................................................................................................... 16
Discussion Questions ........................................................................................................................... 16
Additional Resources ........................................................................................................................... 16
Bibliography ......................................................................................................................................... 18

Security in Afghanistan ............................................................................................................... 22
Overview ................................................................................................................................................ 22
Timeline ................................................................................................................................................. 22
Historical Analysis .................................................................................................................................. 24
Past UN and International Involvement ............................................................................................... 26
   The War on Terror ......................................................................................................................................... 26
   North Atlantic Treaty Organization (NATO) ............................................................................................ 27
Current Situation .................................................................................................................................. 28
   Terrorist Presence ........................................................................................................................................... 28
   Governmental Failures ................................................................................................................................... 29
   Opioids ............................................................................................................................................................. 30
   Foreign Support .............................................................................................................................................. 31
Possible Solutions and Controversies ................................................................................................ 31
   Increased Military Presence ........................................................................................................................... 31
   Governmental Reforms .................................................................................................................................. 32
   Limiting the Opium Industry .......................................................................................................................... 32
   Diplomatic Solutions ...................................................................................................................................... 32
Bloc Positions ........................................................................................................................................ 33
   Major Powers ................................................................................................................................................... 33
   Less Affected States ........................................................................................................................................ 33
   European States .............................................................................................................................................. 33
Discussion Questions ........................................................................................................................... 34
Additional Resources ........................................................................................................................... 34
Bibliography .......................................................................................................................................... 35
Countering Cybercrime

Overview

In the 21st century, war and conflict don’t merely exist in the form of military engagement on land, sea, or air. In a digital age where the world is increasingly more reliant on computers and the internet, technology, though efficient and productive, bears several risks as well. Cyber attacks are becoming more prevalent as technology advances. Consequently, NATO is a victim as well, facing “an average of 500 cyber attacks per month” in 2016.¹

Cyber attacks take place in multiple forms ranging from phishing, an attempt to “dupe recipients to disclosing sensitive data”, to “distributed denial of service (DDoS), where servers are swamped with so much data that they overload and collapse.”² Beyond the destructiveness of cyberterrorism, identifying the perpetrator is difficult as well. In many instances, hackers are completely anonymous and thus hard to track down. Furthermore, the motives behind hackers vary as well. The causes of NATO system shutdowns can range from hacktivism to organized crime and state-sponsored attacks. The variety of cyber attacks is significant because it can indicate the source, motive, and possible area of attack. However, the easy access to anonymity and difficulty in distinguishing cyber attacks makes cyberterrorism much more efficient.

In response, NATO has already implemented several measures against cyber attacks. The establishment of the NATO Cooperative Cyber Defence Centre of Excellence, for example, has researched and improved its data security and those of its allies. Furthermore, NATO has cooperated with the EU through improving cybersecurity and “boosting counter-hybrid capabilities”³ Despite NATO’s many attempts to strengthen its digital security, such measures have not all been successful. Several member states in NATO are more vulnerable because they either lack the infrastructure or knowledge to strengthen their databases. Furthermore, given the rapid and overwhelming nature of cyber attacks, NATO often fails to be agile enough to counter cyberterrorism.⁴ Those who oppose NATO will seek any method possible to weaken NATO’s infrastructure; it is of utmost importance that NATO members cooperate and find a solution.

Timeline

November 2, 1988 — The Morris Worm, one of the world’s first computer worms to be distributed over the internet, is accidentally created by Cornell graduate Robert Tappan Morris. The worm was originally made to gauge the size of the internet; however, a mistake in the production of the worm made it hostile to networks and computers. The Morris Worm set a precedent for hacking as the first major computer attack which led to disastrous effects.

April 2007 — In a dispute with Russia regarding a removal of a war memorial, Estonia falls victim to several crippling cyber attacks on government institutions and infrastructures, which “brought down key financial and state systems.”\(^5\) Analysts explain that such attack was orchestrated by several hundreds of thousands of computers; though there exists no clear evidence proving the perpetrators of such attacks, many pin responsibility on the Kremlin, which the Russian government denies.

May 14, 2008 — Located in Estonia, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established by seven nations: Estonia, Germany, Italy, Lithuania, Latvia, Slovak Republic, and Spain. The organization, in cooperation with the Estonian national defense administration, aims to protect and enhance cybersecurity systems of all NATO member states.

July 20, 2008 — Cyberterrorism in the form of DDoS attacks is used against the Georgian’s internet servers and companies, which crippled its limited internet infrastructure and cut off access to key services in Georgian society. Though there exists no clear evidence that points to the perpetrator, the Georgian government blames Russia, specifically “a shadowy St. Petersburg-based criminal gang known as the Russian Business Network.”\(^6\) Such allegations are denied by the Russian government.

May 10-11, 2010 — The CCDCOE, in cooperation with NATO, held its very first international cyber defense exercise known as the “Baltic Cyber Shield.” 19 nations including Poland and Latvia sent representatives to Tallinn to attempt to defend computer networks under different “cyber-attack-related crisis.”\(^7\) The joint exercise successfully improved cyber defense knowledge on mechanisms of defense and varying hostile attacks.

November 16, 2011 — The United States and Poland officially join the CCDCOE.\(^8\)

January 2011 — Three key departments of the Canadian government — the Finance Department, Treasury Board, and Defense Research and Development Canada — were penetrated by foreign hackers whose IP addresses were located in China. However, there was no clear evidence that China was behind such attacks because hackers could disguise cyber attacks through Chinese servers. These attacks had devastating effects on Canada as hackers gained access to classified data which led to the shutdown of crucial governmental departments.

July 11, 2012 — The NATO Communications and Information Agency (NCI) is established in several NATO member states as a secure platform to “connect the alliance, defend its network, and provide rapid support to NATO operations and missions.”\(^9\) Through surveillance and providing support for the development of cyber security infrastructure, the NCI plays a crucial role in combating cyberterrorism.

February 10, 2016 — Facing similar challenges and threats in online security, NATO and EU cooperated and reached an agreement to counter cyberterrorism together. The NATO Computer Incident Response Capability

(NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU), both establishments that aim to protect their respective organizations from cyber attacks, agreed to exchange information and practices that better protect online networks. Considered a milestone in NATO-EU cooperation, this agreement strengthens the cyber security of both organizations.¹⁰

**June 14, 2016** — In the midst of a contentious US presidential election, Russia, allegedly, involves itself through cyber attacks on the servers of the Democratic National Committee and “stole opposition research on Donald Trump.”¹¹ Hesitant to publicly blame Russia due to fear of the geopolitical consequences, private security companies such as Crowdstrike held investigations into such attacks and revealed that the patterns of the cyber attacks are similar to previous hacks to US governmental institutions.

**May 13, 2017** — Germany’s railway infrastructure was struck by a series of cyber attacks which halted their transportation system. Using legitimate documents such as emails and messages to disguise malicious viruses, the perpetrators of such crimes hid malware within those messages that is immediately triggered when the document is opened. This is a form of attack known as phishing which restricts user access to their own documents; victims must pay up to “$600 to restore access.”¹² No hackers have been identified for these attacks.

**Historical Analysis**

Digital attacks became common in the 1980s as is shown by the release of the Morris Worm in 1988, which was the world’s first computer worm to be distributed over the internet and caused significant damage to over two thousand computers, costing the US Government Accountability Office $100,000 to $10,000,000 and affecting around 6000 computers.¹³ As technology advanced, the methods and efficiency of hackings progressed as well. Historically, hacking was considered a shortcut for programmers to increase the efficiency of computers. In fact, the word “hacker” itself was historically defined as a person who explores, which was attributed to programmers who explored the different parts of computer operating systems. Given that past computing systems were large and inefficient, programmers used hacks to access the internal organs of a computer to increase its efficiency and capability to their needs. However, the reputation of hacking turned for the worse in the 1980s when skilled hackers manipulated computers for their “own questionable gains,” such as the 1989 attack against the US government. The attack came from West Germany and the hackers sold information and software to the KGB.¹⁴

Phone phreaking, a predecessor to current day computer hacking that came about in 1957, is the practice of hacks and manipulations of telephone lines. Phone phreaking rose to prominence in the 1960s and 70s, and set a precedent for the exploitation of technology. In 1957, a young boy named Joe Engressia who has perfect pitch, discovered that “whistling the fourth E above middle C, at a frequency of 2600 Hertz (Hz), would stop a phone

---

call.” John Draper, a hacker involved in the phone phreak community, cooperated with Engressia and discovered that, interestingly, a toy whistle included in boxes of Cap’n Crunch cereal boxes created the same 2600 Hz pitch that could be used to control phone systems. On the basis of a toy whistle, the blue box was developed that was able to control the audio frequencies of the connection between phone operating systems and the phone. This means that a single blue box was able to disguise personal phone lines as operating systems in phone networks such as AT&T and be able to dial to any number that user wishes. In other words, users of the blue box were able to manipulate phone lines and make free calls to any number they desire. Interestingly, Steve Jobs and Steve Wozniak worked on the blue box prior to the establishment of Apple; the two creative inventors even used a blue box to call the pope. However, certain instances of phreaks also had disastrous effects as well. In the 1970s, Draper was able to retrieve the CIA emergency line to the White House and had direct access to President Nixon. Though phone phreaks may seem efficient for phone users, it also had associated harms that allowed owners of the blue box to gain great access to the private lives and information of others.

Hacking groups and organizations rose to prominence quickly in the late 1980s and early 1990s. Many groups existed, ranging from amateur groups such as The 414’s, which only comprised teenagers, to the German hacking organization Chaos Computer Club, which held annual congress meetings that hosted over 12,000 people. Such groups were threatening given their digital capabilities. Despite the young age of the members of The 414’s, “they gained access to different banks, hospitals, and even the Los Alamos Research Laboratory,” which marked the start of an FBI investigation and the prosecution of over 60 charges of computer intrusion. Due to underdeveloped technology at the time, becoming a hacker was more difficult in the past than compared to today. A hacker group was very exclusive and the process of becoming a member was rigorous. This competition in membership raised the standards of hacking abilities of a group, which made their capacity of digital intrusion even greater.

Competition between groups also became a result of various growing hacker groups. Specifically, in 1989, the Masters of Deception (MOD), a notorious hacker group at the time, had a conflict with a splinter group that became the Legion of Doom (LOD); the conflict was known as the Great Hacker War. Internal disputes sparked the beginning of the battle, where simple disagreements between members quickly spiraled into sentiments of animosity and hatred. Their conflict ranged from simple prank calls to disastrous hacks that affected global internet connections and phone lines. Though the conflict was contained between the two groups, the impacts of such battle were felt by American society. Their cyberattacks had disastrous effects on information security; the two hacker groups accessed confidential data such as credit reports and governmental secrets to gain fame.

---

and sell for profit. Eventually, the two groups fell after federal investigations led to the prosecution of several members of both groups, which led to the ending of one of the greatest hacking instances in history.  

Past UN and International Involvement

In the wake of the increasing cyber attacks that are growing in destructiveness, several organizations, in conjunction with private entities, have taken action to fight cyberterrorism through tracing the perpetrators of such attacks and establishing stronger digital security and defense.

International Criminal Police Organization (INTERPOL)

INTERPOL is an international organization that aims to fight transnational crime, including cyberterrorism. Specifically, INTERPOL strives to detect and prevent cyber crimes from occurring through the establishment of “the INTERPOL Global Complex for Innovation (IGCI) in Singapore,” which is a research facility that opened in 2014 that not only investigates cyber crimes and analyzes trends of cyber attacks, but also cooperates with international and private corporations to retrieve and decipher data through information sharing and coordination in its operations. As well, INTERPOL brings together cybersecurity experts to analyze and gather information and trends in regards to cybercrimes, which allows INTERPOL to provide coherent, nuanced intelligence that can be utilized in strengthening a nation’s digital defense. Given that cyberterrorism is an international crime, INTERPOL combats the crime with international efforts.

United Nations (UN)

The United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ), an organ of the UN, has taken several proactive measures to prevent and limit the effects of cyberterrorism through the establishment of clear legislation against cyberterrorism and the distribution of aid in training and infrastructure to help developing states strengthen its cyber security. In particular, UNGA Resolution 65/320 (A/RES/65/320) was adopted by the CCPCJ which aims to “enhance international cooperation” through providing “technical assistance” to counter cyberterrorism. There were many other resolutions other than UNGA Resolution 65/320 (A/RES/65/320) that were adopted by the CCPCJ to address the complex issue of cyber crime.

Private Entities

Though intergovernmental organizations have taken significant steps in advancing cyber security, private, non-governmental actors have played a large role in the fight against cyberterrorism as well. Corporations such as the California based company CrowdStrike, which has contributed to the investigation of cyberattacks during the 2016 US Presidential election, and the UK based corporation Sophos, which has contributed to the defense against the rise of ransomware attacks on the National Health Service (NHS) of the UK, have been vital in the

---


fight against global cyberterrorism. In fact, Kaspersky Lab, a Russian based cyber security company, took part in taking down a destructive malware, Flame, which has been implemented in computers in the Iranian Oil Industry and allowed the users to kill functions of the program that crippled the Iranian Oil sector.

Case Study: The Prosecution of Kevin Mitnick

Kevin Mitnick was one of the most wanted hackers in the world during the 1990s for multiple acts of computer fraud, possessions of unauthorized access devices, and intrusion into governmental departments and companies such as Motorola. He earned a spot on the FBI’s Most Wanted List and was eventually arrested before being incarcerated in February 1995 on a 25 count indictment. Mitnick served more than five years in prison and was eventually released in 2000 and worked in the computer security industry as the CEO of Mitnick Security. The prosecution of Kevin Mitnick is significant given the precedent it set for international attention and for legal action against crimes against computer security.

Current Situation

Types of Cyber Attacks

One of the most common yet destructive methods of implementing malicious software that is capable of data theft and disruption is known as backdoor hacking. In essence, backdoor hacking allows someone to gain full access to a computer; this includes the data on one’s computer. One of the worst incidents of backdoor hacking occurred when a group of hackers known as Equation Group who, allegedly linked to the NSA, infected tens of thousands of Windows Systems, including those of foreign nations such as Syria, Iran, and more.

To gain access to someone’s computer, cyberterrorists often use manipulative social interactions such as a seemingly harmless email or a fake request for personal information to disguise their true intents. Hackers are able to gain full access to one’s computer once the document or software is opened by disguising the virus within trustworthy content. The capabilities of these cyber attacks are so drastic that opening an email could lead to a complete digital hijack by the perpetrator. The use of manipulation to gain access to one’s information is known as phishing. Once a perpetrator gains access to one’s computer, multiple computers are at risk because a single worm can spread to other computers through different networks as well. Conversely, ransomware attacks can be implemented which denies access to any computing functions unless the victim fulfills a demand of the hacker. Such form of attack was used against Ukrainian firms in June 2017, where “the state power company and Kiev’s main port” lost access to its digital information unless a ransom was paid. Such attacks grant hackers significant leverage in holding victims hostage to gain economic profit or information.

---

Cyber criminals can indirectly collect data from others without interacting with their victims’ computer at all. This form of attack works through the use of sniffers, “which works by intercepting and logging network traffic that they can 'see' via the wired or wireless network interface.” Through the use of sniffers, cybercriminals can eavesdrop any information being exchanged between two parties on a network, or retrieve sensitive data such as passwords or authentication tokens as well. One of the most notorious and destructive cases of cyberterrorism occurred through the use of sniffers. In 1990, the United States Department of Defense, NASA, and several other American federal departments were left in shambles by the work of a 15 year old Miami child known as Jonathan James. The underage hacker discovered vulnerabilities in servers based in Dulles, Virginia and was able to install a sniffer with ease, acquiring access to over 3000 messages between NASA staffs and 10 military computers. Through the installation of one sniffer based on a single vulnerability, James stole software and information worth $1.7 million, causing federal agencies to shut down for 21 days and pay over $41,000 for repairs and losses.

Though many cyber crimes are committed with the aim of obtaining data, pure destruction is often desirable for many cybercriminals as well, which can be achieved through distributed denial of service attacks, also known as DDoS. Through overwhelming a sites or program with enormous amounts of traffic and data, perpetrators can make websites and applications completely unusable or extremely slow. DDoS attacks are used against internet distributors to shut down online access to disrupt society, or used against high profile websites as a publicity stunt. Interestingly, in many instances, DDoS attacks are used as a distractor for IT departments or cyber defense systems so cybercriminals can employ other forms of attack to retrieve information. DDoS is constantly evolving and infecting more essential services and applications every day. In fact, cyberterrorists have developed bots that can send DDoS attacks to other computers and networks independently, making these attacks even more drastic and damaging. BBC suffered under the strength of DDoS attacks that were employed by a group known as New World Hacking in 2016. Possibly being one of the largest attacks in history, the DDoS attack against BBC brought down news service as well as other affiliated websites as well. The attack itself reached the strength of 602 Gbps, “almost twice the size of the previous record of 334 Gbps.” Given its simplicity and power, DDoS attacks are frequently utilized by many cyberterrorist organizations. Despite improvements in cyber defense, DDoS attacks persist as one of the most powerful forms of cyber attacks.

Many different forms of cyber attacks are used by cyberterrorists to achieve different aims, whether to gain information and economic profit or to create destruction to increase fear and publicity. Cyberterrorism, regardless of form, has pernicious effects on society and must be understood completely to be countered.

**Difficulties in Fighting Cyberterrorism**

One of the largest challenges faced in the fight against cyberterrorists is attribution. While law enforcement is able to mitigate or even prevent cyber attacks in many instances, cyberterrorism cannot be fully stopped given that identifying the culpable actor is difficult. Cybercriminals can stay anonymous with ease by using private networks to communicate and creating fake identities to stay hidden, which allows cyber attacks to persist when

---

defense agencies are unable to track and shut down cybercriminal organizations. As well, cyber crimes are committed in a transnational manner, which means that indication of culpable actors becomes more difficult given the much larger scope of potential suspects.

Even in instances where an attack can be attributed to a culpable perpetrator, there still exists ambiguity in the exact identity of a hacker because motives are significantly different between different types of hackers. Though all forms of cyberattacks can be damaging, understanding the different ways different hackers attack is crucial in the fight against cyberterrorism as well.

**State-sponsored Attacks**

Geopolitics and the competition for global hegemony have existed since the dawn of civilization, but are fought through modern techniques today. Countries who are self-interested often employ the use of cyber attacks to retrieve sensitive data such as intellectual property, state secrets and more for their own gains. The prime example of state-sponsored cyber attacks are attacks launched by China, who intruded several business networks to illicitly gain intellectual property and executive communication in order to strengthen its own state own enterprises. In many instances, states employ private, less known groups to perform such attacks, such as Group 61398, who have been hired by the Chinese government in many instances to steal trade secrets from companies such as "Westinghouse and US Steel."

**Criminal Organizations**

Cybercriminal organizations are becoming more prevalent in today’s increasingly digital world. Given rapid developments in technology, the ease of entry into hacking, through learning the fundamentals, has become easier, making it a more desirable, profitable venture for many digital mobs to pursue. Moreover, given increased reliance on technology throughout society, cybercriminal organizations hold significant power in the digital world; one attack on infrastructure could have disastrous effects on several other connected institutions. Through obtaining sensitive data and private information, cybercriminal organizations profit at rapid rates through selling these data. As well, cybercriminal organizations also utilize cyberterrorism to perform other crimes, such as the distribution of drugs or illegal weapons through digital means. Perhaps modern criminal organizations no longer exist on the streets, but their potential for destruction stays consistent in the digital world.

**Hacktivism**

Efforts in activism have changed from ground based revolutions or protest sit-ins to dissent and discourse online. The legitimacy of hacktivism is heavily debated; some argue that it empowers people by exposing information that people should have a right to access, while others argue that hacktivism utilises tactics that create societal harms which makes its cause illegitimate. The justification of hacktivism lies in a gray area. Though most would support examples of hacktivism that targets corruption or promotes free speech, such as the cyber attacks against the Ferguson Police system after the shooting of Michael Brown, cyberterrorism, with more malicious aims, is

---


often confused with hacktivism.\textsuperscript{36} Cyberterrorists, though also promoting a cause, often function in ways that cause significant financial and even human costs.

Possible Solutions

Cyber Weapons

The best form of defense is offense. Cyberterrorists and criminal groups aren’t the only actors who are capable of using technology in their favor; law enforcement and defense agencies can as well. The use of cyber weapons, some argue, has incredible efficacy given it weakens the most powerful tool that cybercriminals have — technology, evident in Stuxnet, a computer worm that was able to halt Iran’s nuclear weapons program.\textsuperscript{37} Furthermore, states can gain information regarding terrorist groups through engaging in cyber combats, as well as avoid traditional means of counterterrorism which breeds more external harms. Conversely, others claim that giving states the right to use cyber weapons offensively is a breach of their power. Given that no state is perfectly accountable, giving them such immense power could result in unaccountable uses of it as well. Furthermore, opponents claim that using cyber weapons would only encourage cyberterrorists to amplify their attacks in frequency and magnitude, causing more harm and conflict.

Increased Surveillance/Restricted Online Access

Cyber attacks can only thrive on the existence of the online world. Necessarily, limitations on online infrastructures increase the difficulty at which cybercriminals can operate. Proponents for increasing government surveillance and restricting online access claim that such government actions would create an effective deterrence against criminal groups from committing cyber crimes through increasing the chance of being caught and limiting the space in which they operate.\textsuperscript{38} However, opponents argue that such restrictions and surveillance is a violation of people’s privacy and individual rights. Furthermore, opponents claim that this would be ineffective because cybercriminals would simply move to private networks such as the dark web that isn’t regulated by states at all.

Increased NATO Presence and Support

While cyberterrorism is a global epidemic, certain states are disproportionately affected by the malicious effects of cyber attacks. Countries such as Estonia or Georgia, who are geographically more vulnerable to state sponsored attacks, or Bulgaria and Albania, who are more vulnerable to cyber attacks given their developing status, cannot often defend themselves digitally. Increased NATO funding and support, similar to the construction of the CCDCOE in Estonia, would allow poorer states to invest more in strengthening its cyber defenses through improving “virus scanners, intrusion prevention technology, and forensic software.”\textsuperscript{39} In addition, the increased NATO funding to developing states would actually be profitable in the long term because more developed states are able to allocate funding to its military or external organizations such as NATO. However, many opponents argue that many NATO members are becoming more reliant on more developed


states such as the US and have grown complacent in supporting NATO. Giving these states more NATO funding and infrastructure would only exacerbate this imbalance in contributions even more. Moreover, reliance also becomes problematic when states must combat cyberterrorism independently, even in the absence of NATO support.

**Cooperation with Private Entities**

While governmental actors bear significant obligations in the fight against cyberterrorism, private entities such as companies and firms have significant stakes in this issue as well. In a more digital world, private companies such as Google and Facebook hold significant portions of information and data that are sought after by cybercriminals and cyberterrorists. Thus, state cooperation with private entities is imperative in combating cyberterrorism. Proponents of such a partnership argue that the fight against cyber attacks becomes significantly easier when private entities can distribute data to states, which allows them to better analyze and investigate patterns and processes of cyber attacks, leading to improved forms of prevention and mitigation of cyber attacks. However, opponents argue that, on a legal and ethical level, states shouldn’t have the power to demand private entities for information, not only because it is a violation of the rights of private institutions, but also because it is a violation of the rights of individual users who never consented to governments accessing their information. Furthermore, opponents claim that such cooperation is actively damaging to the reputation of a corporation as well.

**Bloc Positions**

**Baltic States**

Given their regional proximity to Russia, the Baltic states are disproportionate victims of state-sponsored cyber attacks, making their governmental institutions and infrastructures more vulnerable. The Estonian defense minister, Jaak Aaviksoo, has said that “[Estonia] clearly feels [cyberterrorism] as a threat to national security.” Given the threat of cyber attacks, Eastern European states such as Latvia and Albania urge strong support and defense against cyberterrorism and potential attacks.

**European States**

European states such as Greece and France are victims of cyberterrorism mainly from individual actors rather than states. In fact, as members of the European Union (EU), European states have established the Internet Referral Unit, as part of Europol — the law enforcement agency of the EU — to “remove jihadist content from the internet.”

---


The Danish government, which has also been under cyber attacks, stated that: “Recent years have seen a significant rise in the number of attempted cyber espionage attacks against Denmark and Danish interests. There were several campaigns launched in 2016 by foreign states targeting the Danish central administration and other public authorities, to access information regarding current Danish foreign and security policy.”

**Major Powers**

Major powers such as Canada or Britain take strong stances against cyberterrorism, labeling it as one of the biggest threats to national security. They have already taken proactive and defensive measures such as establishing cyber defense teams. Other major powers such as the United States and Italy are tackling cyber attacks head on, which is disproportionately aimed at private and governmental institutions. As well, Germany established a programme called the Strategic Technology Initiative (SIT), which Steffen Seibert, Angela Merkel’s spokesman, describes as “an early warning system so that Germany for the first time will be in a position to identify attacks on the German IT infrastructure.”

**Discussion Questions**

1. What are the different motives behind cyberterrorism?
2. How do the effects of different cyberattacks differ in impact?
3. Is the current response to cyberterrorism adequate?
4. What impacts do cyberattacks have on governments and societies?
5. What are NATO and other international organizations’ roles and capabilities in countering cyberterrorism?
6. Should the response to cyberterrorism be more aggressive, in the use of cyber weapons, or be more defensive, in establishing stronger defense on digital networks and technology?
7. What are the roles of private actors such as corporations in cyberterrorism?
8. What are the roles of developed states to support developing states that are disproportionately vulnerable to cyberattacks?
9. How has technological advancements changed cyberterrorism and defense against cyberterrorism?
10. How has the increased reliance on technology affect people’s everyday life?

**Additional Resources**

Article on the impacts of cyberterrorism on India-Pakistan Relations:


---


45 Wagstyl, S. (2014, November 11). Germany plans early-warning defence against cyber attacks. Retrieved July 28, 2017, from [https://www.ft.com/content/54ce1fea-68f2-11e4-b389-00144feabdc0](https://www.ft.com/content/54ce1fea-68f2-11e4-b389-00144feabdc0)
Video on how cyberterrorism has changed modern terrorism:
https://www.youtube.com/watch?v=CNfNvhWlH7M

Powerpoint on the UN’s analysis of cyberterrorism:

Video on the process and effects of hacktivism:
https://www.youtube.com/watch?v=ylZcsv86Uiw
Bibliography


Security in Afghanistan

Overview

In the modern age, terrorist groups such as the Taliban and Al Qaeda are still rampant in many parts of Afghanistan despite the death of Osama Bin Laden. NATO has vested interest in stopping these groups from growing in size and power, evident in the launch of NATO-led security mission — the International Security Assistance Force — in 2003. However, a stronger NATO response is necessary with the recent rise of terrorism and power within such radical groups.

Currently, the attempt to fight the Taliban by the Afghan National Security Forces has resulted in increased casualties and violence. The conflict within Afghanistan leans in favor of terrorists due to structural problems that exist within Afghanistan’s security force, such as corruption and lack of funding. Regions such as the “provincial capital of Kunduz and multiple districts of Helmand” have fallen under Taliban control, but the Taliban isn’t the only Islamic group in Afghanistan. The Middle Eastern state is divided into multiple splinter groups, such as Pakistani militants, Lashkar-e-Taiba, and Tehrik-e-Taliban-Pakistan. Furthermore, the Taliban is able to sustain its power because it controls multiple opium poppy fields that provides capital; the Taliban also grants jobs and basic needs to individual Afghans which increases its legitimacy as a group. The rise of terrorism in Afghanistan has tremendous effects on the livelihoods of innocent Afghans as well as the Middle Eastern region, given that it has effects on neighboring states such as Iran, Pakistan, and possibly Turkey.

Despite efforts taken by NATO to counter terrorist groups in Afghanistan, Taliban resurgence and violence has magnified, especially after the formal ending of the International Security Assistance Force in 2014. Many call for increased NATO presence in Afghanistan, but this solution is also faced with vast criticism and controversy. It is of utmost importance that delegates explore the many different factors that contribute to the instability in Afghanistan as well as the different solutions that can be chosen to address it.

Timeline

1979-1989 — In the midst of the Cold War, the CIA funded Afghan rebels, known as the Mujahideen, to fight against the USSR invasion of Afghanistan by providing arms and training; this US operation program was known as Operation Cyclone. Despite successful efforts in the fight against Afghan communism, the Mujahideen later splintered into the many jihadist groups present today, such as the Taliban and Al Qaeda.

1994-1997 — Given the failure of the communist regime in Afghanistan, the Taliban, under the leadership of Mullah Mohammed Omar and Islamic students trained in Afghan and Pakistani madrassas, sought power through taking up arms. The movement was successful in overtaking Afghanistan through capturing major cities

and implementing a strict set of Islamic law, as well as creating a safe haven for terrorism—giving sanctuary for Osama Bin Laden and his followers to plan attacks against the US.⁵⁰

**September 11, 2001** — Al Qaeda, under the leadership of Osama Bin Laden, launched one of the deadliest terrorist attacks in history through hijacking four commercial airplanes that were crashed into the World Trade Center and the Pentagon, resulting in nearly 3000 deaths and the collapse of the World Trade Center.⁵¹

**October 7, 2001** — In response to the September 11th attack, the US, under the leadership of George W. Bush, officially began the War on Terror through the employment of Operation Enduring Freedom. Through the use of airstrikes and cooperation between different nations such as Italy and Spain, the operation was successful in toppling the Taliban regime—although Taliban resurgences still occur throughout Afghanistan.⁵²

**August 2003** — Given that the September 11th Attack triggered NATO’s article V of collective defense, which states that an attack against one member state is an attack against all allies, NATO employed the International Security Assistance Force (ISAF) which sent over 130,000 troops to conduct security operations throughout and improve Afghanistan’s domestic security.⁵³

**October 9, 2004** — Hamid Karzai, who was one of the previous heads of an interim government after the fall of the Taliban, was democratically elected as the leader of Afghanistan. Though Karzai introduced reforms to Afghan society, the Taliban was still a power group with domestic hegemony in different parts of Afghanistan.⁵⁴

**July 21, 2005** — Al Qaeda launched a failed attack in London, attempting to disrupt London’s public transport system. Fortunately, the explosives failed to detonate, leading to only one minor injury but no loss of life. The four suspects were arrested eight days later.⁵⁵

**April 23, 2013** — Mullah Mohammed Omar died of “health problems at a hospital in Pakistan,” creating a power vacuum in the leadership of the Taliban.⁵⁶

**January 1, 2015** — Following the conclusion of the ISAF at the end of 2014, NATO employed the Resolute Support Mission (RSM) to further stabilize and assist Afghanistan in security. The missions entail funding for the military personnel of Afghanistan, creating transparency and accountability in its government, and other forms of support.⁵⁷

---

Historical Analysis

Islamic terrorism within Afghanistan began in earnest during Afghanistan’s transition from a monarchy to a republic in 1978. The People’s Democratic Party of Afghanistan (PDPA), a Marxist political party under the leadership of Nur Mohammed Taraki, staged a coup and took over Afghanistan on April 27, 1978. Despite its wide range of support during the revolution, the ruling party faced increasing resentment due to its socialist policies and anti-religious reforms that weren’t accepted by Afghans accustomed to its traditional social system. Subsequently, Afghanistan saw the rise of a guerrilla Islamic military group known as the Mujahideen in opposition of Afghanistan’s communist government. The communists maintained control throughout major cities, which led to the Mujahideen basing its support and power in the countryside. This triggered the brutal and violent Afghan War.

Battles quickly amplified in destruction after the USSR, supporting the PDPA, and the USA, supporting the Mujahideen, established their presence in the Afghan War. Conflicts quickly escalated as tactics such as bombing rural areas and using aircraft missiles were introduced, forcing many innocent, Afghan citizens to seek asylum in Iran and Pakistan. In addition to US funding, the Mujahideen also had an elaborate structure in recruitment. Osama Bin Laden, who was a member of the Mujahideen at the time, established the Maktab al-Khidamat (MAK), also known as the Services Office, with his mentor, Sheikh Abdullah Azzam, to recruit fighters for the Mujahideen. The MAK was small at first, only attracting a couple members and having limited funding; however, the MAK gradually gained traction as foreign donors, including the CIA, the Saudi government, and the Pakistani Inter-Services Intelligence, funneled supplies and funding into the organization. The MAK was eventually able to establish bases internationally, even in cities such as Brooklyn and Tucson. Through the increase in foreign support and domestic instability in the USSR, the Mujahideen succeeded and the Soviets withdrew.

Despite the Mujahideen victory in Afghanistan, the Islamic guerilla organization was still a fragmented group of independent militias that splintered into several guerilla organizations. Following a period of instability, Mohammed Omar, the founder of the Taliban, took over Afghanistan. Omar was born in the Kingdom of Afghanistan in the 1950s. Omar was an ethnic Pashtun, the predominant ethnic group in Afghanistan, who was raised in Islamic environments and attended Islamic schools known as madrassas to advance his studies. Throughout his life, he fought with the Mujahideen against the Soviet invasion and established a madrassa himself following the Soviet withdrawal from Afghanistan. In 1996, Omar led a group of students to take over different cities, such as Kabul and Kandahār, in Afghanistan and formed the Islamic Emirate of Afghanistan, with the support of countries such as Pakistan, Saudi Arabia, and the UAE. The Taliban envisioned a restrictive Islamic society. Socially conservative policies were implemented under Taliban rule, including strict dress codes.

---


Vancouver Model United Nations 2018 24
and limitations in any form of media. Moreover, females particularly suffered under Taliban rule, evident in the crackdown on any female who wished to go to school or even appear in public without a male escort.\textsuperscript{63}

People not only suffered domestically, but also in neighboring or Western states as a result of the numerous attacks launched by the Taliban. The Taliban wasn’t deterred in its attacks despite international military intervention and sanctions. Besides the plethora of bombings of embassies and public infrastructure, the Taliban’s most notorious attack occurred in the early 2000s when several commercial airplanes were hijacked to be flown into the World Trade Center and the Pentagon, commonly known as the September 11th Attack.\textsuperscript{64} The attack was largely carried out by Al Qaeda, but the Taliban was complicit in aiding Al Qaeda in the process. More specifically, the Taliban provided a safe haven for Osama Bin Laden during its reign in Afghanistan to create a network of terrorists and cement radical Islamic beliefs in Afghan society. The Afghan government protected him extensively despite numerous attempts to extradite him.\textsuperscript{65}

Osama Bin Laden was born in Riyadh, Saudi Arabia and founded Al Qaeda based on Pan-Islamic beliefs, which seek to create a united Islamic world in the Middle East through jihad, also known as a holy war. Bin Laden, similar to Omar, was raised in an Islamic environment, studied under madrassas, and even joined the Islamist Muslim Brotherhood. His history of Islamic military groups began with Mujahideen, particularly the establishment of the MAK which strengthened the Mujahideen significantly. Following Soviet withdrawal from Afghanistan, Bin Laden and Azzam returned to Saudi Arabia to establish Al Qaeda, a militant Sunni Islamist organization that bases its legitimacy more on symbolic acts of terror rather than military campaigns. The initial reactions to Al Qaeda were largely resentful, evident in both Saudi and Sudanese expulsion of Bin Laden. The deportation angered Bin Laden, which led to more aggression in Al Qaeda attacks, including the attempted assassination of Egyptian president Mubarak.

Bin Laden eventually sought refuge in Afghanistan and cooperated with the Taliban to launch several attacks, including bombing US embassies and American Naval ships.\textsuperscript{66} Al Qaeda was effective in recruiting members despite government resentment against the Islamic militant group. Similar to the MAK, Al Qaeda deployed numerous agents and bases internationally to seek new members and gain information. Moreover, Al Qaeda provided incentives to join the organization, which meant many individuals were seduced by financial and social incentives, especially those who belong to lower socioeconomic class. However, Al Qaeda’s recruitment method is coercive in many instances as well. In particular, Al Qaeda members often preach Islamic ideals and beliefs to potential recruits and persuade them to believe in the jihad, particularly targeting people who suffer from drug addictions or mental complexities.\textsuperscript{67} Al Qaeda and the Taliban had immense destructive capabilities together, domestically and internationally. It was up to the rest of the international community to step in.

Past UN and International Involvement

The War on Terror

Following the September 11th attack, President George W. Bush officially began the War on Terror, which seeks to defeat senior members of Al Qaeda and other terrorist groups, weaken fundamental structures of Islamic militant organizations, and preserve the security of the international community. The War on Terror was mainly fought in Afghanistan, though operations were deployed in Iraq, Pakistan, and Yemen as well. Operation Enduring Freedom, which was the operation in Afghanistan, was quickly implemented after the September 11th attack and proved to be effective. The USA, along with other supporting nations such as Canada and the UK, formed coalition forces that fought Taliban control in the region. The international community fought with ground troops, air strikes, and any means to stop the Taliban. The US was successful and took back cities such as Kabul and Kandahār by December 2001. Subsequently, Hamid Karzai was elected president of Afghanistan in 2004.  

A key strategy of the US military was the use of targeted killings to counter terrorist groups; for example, under the Obama administration, the US deployed numerous drone operations that targeted specific individuals, usually senior members of terrorist groups or other wanted targets. Targeted killings were effective given that most terrorist groups were structured hierarchically, which meant that taking out the leader effectively disrupted and disabled terrorist groups, leading to internal instability and splinters. The first person to be killed by US targeted strikes was Anwar al-Awlaki, a Yemeni senior recruiter in Al Qaeda. The US didn’t fight this war independently; through several covert operations that were carried out in Afghanistan, the US was effective in training local Afghan resistance forces that countered Taliban attacks and retrieved intelligence as well. On May 2nd, 2011, US Navy SEALs in Abbottabad, Pakistan raided the house of Osama Bin Laden, leading to his death.

However, the War on Terror is not without its problems as well. Many critics of the war challenged the true purpose behind the War on Terror. Though the US claims that the War on Terror is justified in the pursuit of global security and preservation of human rights, many claim that the US is involved in the Middle East to advance its economic interests and political interests by controlling the region’s rich resources and strengthening its global hegemony respectively. In addition, the War on Terror has significant human costs, not only through the destruction of infrastructure and the killing of innocent lives (at least 52,000 Pakistanis have been killed since 2004), but also direct killings and kidnapping of many suspects without fair due process. In addition, unaccountable practices in warfare also bred more anti-Western sentiments, incentivizing more individuals to sympathize with terrorist groups and participate in them. Another criticism against the War on Terror was the use of enhanced interrogation techniques - torture; tactics such as waterboarding, prolonged isolation, and sleep deprivation, all of which considered basic human rights violations, were utilised in US secret prison camps such

---

as Abu Ghraib and Guantanamo Bay. Though the War on Terror faced much domestic criticism in the US as well, given the significant financial costs of sending ground troops and using airstrikes. Though the War on Terror is effective in certain instances, many opponents of the war claim that all of its human and social costs outweigh its benefits.

**North Atlantic Treaty Organization (NATO)**

Following the September 11th attack, a precedent was set when NATO triggered Article V for the very first time and activated its collective defense clause. NATO led the International Security Assistance Force (ISAF), which was originally established by Security Council Resolution 1386 (S/RES/1386) in 2001 until NATO took over in subsequent years. Though the main contributors included the US and UK, many other NATO members and allies contributed to the mission as well, evident in the presence of 1900 French troops under the ISAF as of 2008. The ISAF had many objectives in Afghanistan; though the Taliban is no longer in power, insurgencies are frequent in rural parts of Afghanistan and even major cities such as Kabul. When the ISAF first appeared in Afghanistan, it largely centered its defensive capabilities in the Afghan capital. Gradually, the ISAF increased its presence throughout Afghanistan, establishing numerous military bases in different parts of Afghanistan such as Herat, Bagram, and Mazar E-Sharif. Each headquarter was led by different military commanders with their own troops and resources under their jurisdiction, allowing them to fight and establish defenses against insurgencies in each Afghan region. In addition, the ISAF enacted long term tactics for fighting terrorism by providing training and funding to the domestic Afghan military force, ensuring that Afghanistan can independently counter domestic threats.

However, ensuring security in Afghanistan entailed much more than eliminating the threats of terrorism. Following the fall of the Taliban regime, the creation of a power vacuum and destruction in infrastructure were all systemic problems that plagued Afghan society, which led to the Bonn Agreement. The Bonn Agreement was a series of negotiations and agreements intended to structure the recreation of the state of Afghanistan following the fall of the Taliban regime. Through international support, the Bonn agreement established a refined constitution and legal framework, created an interim government and system of democratic representation, and laid the foundation for the UN, NATO, and foreign aid to Afghanistan in its transition to a more stable nation-state.

Though the ISAF was effective in suppressing terrorism in Afghanistan, the ISAF was met with criticisms as well. Opponents criticised NATO for its limited presence in Afghanistan, claiming that terrorism in rural regions is a far more pressing, yet, unaddressed issue. Furthermore, NATO was criticised for the escalation of conflict as well. Though an increase in troops and arms enhanced NATO’s ability to counter terrorists, it also led to an

---

increase in collateral damage and destruction, something that is criticised by human rights activists and other opponents who claim that demilitarisation should be a prioritized objective. The Bonn Agreement was met with criticisms as well because many of its objectives — the implementation of legal frameworks and democratic elections — weren’t established and implemented properly, which led to corrupt, unaccountable practices that is rampant in the Afghan government.79

Current Situation

Terrorist Presence

Presently, approximately “60 percent of the total districts in the country are under government control and the remaining 40 percent remain under the Taliban or under the control of other armed groups.”81 Afghan society is still plagued with frequent suicide bombings that are often targeted at NATO headquarters, embassies of Western states, and even civilian districts. Conflicts have intensified recently; incidents of injuries and casualties occur on a daily basis.82 In addition, Afghanistan has seen an increase in different terrorist groups given the recent rise of terrorism globally. Al Qaeda is still very prevalent through Afghanistan, recruiting young Afghans

and training its future fighters on a daily basis alongside the Taliban. Afghanistan is still in some ways a sanctuary for terrorists to manifest and plan its attacks. The Islamic terrorist group strengthened its regional influence in recent times, cooperating with Al-Nusra and Hezbollah in Syria and Lebanon respectively.\(^83\) In addition, many smaller terrorist groups have made their presence in Afghanistan, such as the Lashkar-e-Taiba and Lashkar-e-Janghvi, both from Pakistan. Some groups cooperate with each other while others are rivals of each other; regardless of the relationship between different terrorist groups, they all pose a danger to the stability of Afghan society.\(^84\) Currently, US and NATO presence is minimal compared to the early 2000s due to domestic pressure to end foreign conflicts. NATO and the US currently have 21,859 troops in Afghanistan; though its offensive capabilities are reduced in the short term, NATO has focussed its support on creating long-term independent resistance in Afghanistan. Its current mission, Resolute Support, “provides training, advice, and assistance to Afghan security forces and institutions.”\(^85\) However, terrorism is still rampant due to multiple factors.

Governmental Failures

Afghanistan suffers from the inherent corruption that is ingrained within its government, as seen on the Transparency International’s Corruption Perception 2015 index (Afghanistan ranks 166 out of 168 countries).\(^87\) Many politicians have become more self-serving and concentrate power and resources within the corporates and

---

upper-class. In addition, ethnic divides in Afghan society mean that politicians are often biased toward their own cultural groups, creating more obstacles in a functional government that represents all. Consequently, humanitarian aid and foreign donations, including the billions of dollars that the US has spent on rebuilding Afghanistan, are consumed by corruption and unaccountable practices. Corruption not only harms innocent Afghans, but also give them a greater incentive to join terrorist organizations that are effective at marketing themselves as an alternative means of living, bolstering the strength of terrorist groups.88 In Taliban controlled areas, though it provides basic access to hospitals and schooling, the terrorist group still installs vast Islamic laws and restrictive ways of life.89 Terrorist groups in rural areas also persistently maintain their legitimacy through the use of propaganda, teaching Islamic beliefs in its madrassas or fostering hate against Western states, both of which are effective in creating psychological control of its members and spreading its influence. In addition, many parts of Afghanistan such as Faryab and Balkh in the North have significant regional control by local warlords as well. Individuals with control over their own militias, such as Atta Mohammad Noor and Abdul Rashid Dostum have hegemony over regions as well, making the federal government more decentralised and less capable.90

**Opioids**

Afghanistan is the world’s largest producer of opium; more than 90% of the global heroin trade originates from Afghanistan. Subsequently, it is no surprise that terrorist groups and militias participate in this industry as well. Despite the government’s attempts to crack down the opium production industry, systemic corruption halts the government because many local commanders and officials directly profit off of the production of drugs as well. In addition, areas controlled by militia and terrorist groups foster the opium production industry, providing protection and goods to farmers who grow heroin.91 Opium production in Taliban controlled regions, such as Kandahar and Uruzgan, have earned the Taliban a $400 million USD profit from 2011-2012.92 In addition, given that drugs intrinsically are addictive, there are incredibly high demands for increased supplies of drugs which allow the terrorist groups and militias to earn more profit.93 The wealth gained by the Taliban is largely used to mount attacks and fund weaponry to strengthen its military power.94

---

Foreign Support
Insofar as the Afghan military force has received support from Western states and NATO, opponents of the Western bloc have solidified their support for terrorist organizations as well. Iran, a known opponent of Western states, has, allegedly, funneled support and arms to terrorist groups in Afghanistan to fight Western presence. Specifically, US intelligence war logs have claimed that Iran has offered monetary rewards for members of militias who kill Afghan soldiers and government officials. In fact, many of Al Qaeda’s car bombings and attacks can be partly attributed to Iranian support. Given pre-existing geopolitical tensions between Western states and certain Middle Eastern states, those who oppose the west have an incentive to fight Western states’ presence in Afghanistan, conveniently through existing militias and terrorist groups. In fact, there is also evidence that suggests Russia, unlike its historical support for the state, also indirectly supported terrorist groups such as the Taliban. In addition, Russia is advancing its own hegemonic interests through funding such groups as well. Through foreign support, terrorist groups and militias in Afghanistan pose significant threats to domestic and global security.

Possible Solutions and Controversies

Increased Military Presence
Given that the current presence of several terrorist groups in Afghanistan with increasing insurgencies harm the daily lives of Afghan citizens, increased military presence is perhaps the most forceful measure that NATO could take to counter terrorism in Afghanistan. More aggressive forms of military action allow NATO to be more assertive in fighting terrorists in Afghanistan, in contrary to its current defensive stance. Home-grown resistance may not be possible given the structural problems that are ingrained within the Afghan government. Foreign action, given the powers and capabilities of the international community and organizations, can have much more significant impacts on fighting terrorism in Afghanistan. In fact, many countries have contemplated increasing troop presence in Afghanistan. The advancement in military technology in nations such as the US and UK plays a significant role in limiting the powers of the Taliban through using targeted strikes that take out its leaders or bombing campaigns that disrupt its supply chain. Given its efficacy, military presence can be very effective in stopping hostile insurgencies in Afghan society.

However, military presence is a solution met with controversy as well. Those opposed to militaristic solutions claim that the accountability in warfare is often unchecked, leading to atrocities and violence being committed by the very soldiers that were sent to protect the innocence. Powerful Western states’ ability to get away with committing horrific acts of warfare, as countries such as the US has done historically in the Iraq War and the Korean War, is tremendous and increased military presence would allow them to further that. Furthermore, unaccountable acts are not only counterproductive in fighting terrorism, but also give far more legitimacy to

---

terrorist groups who can now scapegoat Western states while bolstering their credibility as organizations. Many individuals, out of hatred for Western states and their atrocities, actively choose to terrorist organizations. Finally, increased military presence would escalate conflict, create more chaos and violence, and cause unnecessary damage to innocent lives and basic infrastructure.

**Governmental Reforms**

A key step in reforming Afghanistan is to fundamentally change the government to be more sustainable and accountable. Currently, the Afghan government, especially under the leadership of President of Ashraf Ghani who aims to counter corruption, has already established several committees such as the National Procurement Authority (NPA) to investigate certain governmental officials and actions. Tackling government corruption would aid the fight against terrorism, not only by making governments more accountable and efficient, but also making people trust the Afghan government more, incentivizing less sympathy for terrorist groups. However, governmental reforms are difficult given that the Afghan government is deeply entrenched in corruption and bias, which makes this solution difficult to implement in practice in comparison to other solutions.

**Limiting the Opium Industry**

Terrorist organizations profit significantly due to the high demand for drug usage globally and domestically. Given the addictive nature of such narcotics, distributors are capable of setting the price as high as they wish because addicts are coerced into continually purchasing them. Historically, the War on Drugs has had its benefits in limiting the economic powers of cartels and militias, creating more difficulty for such groups to strengthen. However, the War on Drugs has been highly criticized as well, given many of its failures and counterproductive harms. Specifically, the War on Drugs saw DEA agents militarily shut down and destroy opium fields, which indirectly harmed farmers who relied on the industry as a way of economic sustainability. In addition, the War on Drugs pushed the drug industry to unregulated black markets, where the process and distribution of drugs is far more discreet and unknown to international organizations and domestic governments. Though countering the opium trade in Afghanistan is a noble goal, the methods used to fight such a war historically have failed and worsened situations in Afghan society.

**Diplomatic Solutions**

Negotiations can often be the most desirable solution given its peaceful nature. If a compromise could be reached by the international community, the Afghan government and terrorist groups who often have political aims, could minimize conflicts. In addition, giving some legitimacy to terrorist organizations can be beneficial as well. Not everyone in the Taliban or Al Qaeda are radical Islamists; given that these organizations offer forms of social and financial support, many individuals join terrorist militias as a way of mere survival. Giving some legitimacy to terrorist groups can be beneficial to those who are coerced to be a part of such organizations as well. Though diplomatic solutions are beneficial in many ways, they are idealistic and unrealistic as well. Diplomatic solutions have been attempted in the past between NATO, Afghanistan, and the Taliban, but have failed because no compromise could be reached. The Taliban expected all NATO troops to leave Afghanistan while NATO expected Taliban to surrender certain senior members of its groups, neither of which could be agreed upon.

---


Both organizations had high demands which the opposing actor couldn’t meet. Even if some form of agreement could be reached, terrorist organizations are not trustworthy. The possibility that such groups could attack again is high and especially devastating when Western states and national governments are under the assumption that these groups are demilitarised. Despite its benefits and effectiveness, diplomacy faces problems in many ways as well.

**Bloc Positions**

**Major Powers**

Many Western nations, such as the US, have been victims of terrorist attacks. These nations, given their capabilities and state, intend to respond to terrorism with significant force. In fact, in response to the increased Taliban insurgencies, H.R. McMaster, a US national security advisor, has stated that “it’s time for us, alongside our Afghan partners, to respond.”\(^{102}\) Nations that have been disproportionate victims of terror tend to support increased troop presence, enhanced use of drone strikes, and other aggressive military solutions to fight terrorism through any means possible. In addition, major powers have cooperated with domestic Middle Eastern states in the fight against terrorism, evident in America’s cooperation with Iraq. Cooperation between these states have proven to be effective because developed major powers can provide equipment and technology while domestic Middle Eastern states can provide intelligence and information; the combined effort targets terrorism far more effectively than isolated efforts.\(^{103}\)

**Less Affected States**

Countries such as Canada or Italy, though less affected by the atrocities of terrorism, are still very much committed to the fight against the Taliban and other terrorist militias. As members of an organization based on the principle of collective defense, these states have a responsibility to fight hostile enemies and but not engage in overly aggressive militaristic tactics as well. However, support for stability can come in many forms. These countries have played more secondary roles in the fight by supplying troops when necessary and providing more defensive forms of support in facilitating security in Afghanistan. Furthermore, these nations have always provided humanitarian aid to innocent Afghans who suffer under the violence and instability, making it less likely for them to join terrorist organizations for survival.

**European States**

Countries such as Germany or Greece, though not as affected by the impacts of terrorism, are largely affected by the disproportionate indirect harms as a result of instability in Middle Eastern states. The impacts of terrorism have significantly increased refugees and asylum seekers, particularly in Europe. In fact, in 2015, Afghan citizens who left Afghanistan due to increased Taliban attacks comprise “18% of the some 387,000 who arrived on Europe’s shores via the Mediterranean.”\(^{104}\) As a consequence, the significant effects of refugee intake in Europe incentivizes these states to take action to limit the direct impacts of terrorism. Major European powers such as

---


Vancouver Model United Nations 2018 33
Germany and France can afford to take more aggressive actions such as increased troop presence and air strikes while smaller European states such as Estonia and Slovakia contribute less, but proportionally. In addition, many European states have taken a more reactive approach in the fight against terrorism, regulating gun control and tightening screening processes in immigration. Defensive tactics to mitigate the impacts of terrorism works well in conjunction with active approaches as well.  

Discussion Questions

1. How has historical solutions and factors contributed to the state of terrorism in Afghanistan today?

2. What is the significance in noting the differences between terrorist organizations in Afghanistan?

3. What are the tactics used by terrorist organizations to conglomerate its power and how can NATO stop them?

4. What are the international effects of terrorism and what is the role of NATO and the international community in stopping terrorism?

5. How have domestic solutions in Afghanistan worked in the fight against terrorism and how can they be improved?

6. How has the use of propaganda and radicalization affected the recruitment capabilities of terrorist organizations?

7. How should the international community approach and portray terrorist organizations?

Additional Resources

Video on the history of the Taliban:
https://www.youtube.com/watch?v=s9j1H330Nmo

Video on NATO presence in Afghanistan:
https://www.youtube.com/watch?v=yEQYsP_YmGQ

Video on Islamic terrorism and radicalisation:
https://www.youtube.com/watch?v=ugK61au1dV0

NATO analysis on its current mission in Afghanistan-Resolute Support:

Article analysis of society under Taliban rule:

Bibliography


