**Forum:** General Assembly Third Committee

**Issue:** Countering Terrorism in a Digital Age

**Student Officer:** Yuxuan Xu

**Position:** Deputy President of the General Assembly Third Committee

Introduction

In an unprecedented era of international diplomacy, terrorism has emerged as one of the gravest threats to international security, particularly for poor or persecuted individuals. Popularized in the 1970s, the term terrorism broadly refers to the unlawful use of violence or intimidation against civilians. Large scale organized violence directed against civilians has been on a rise since 1980, which eventually culminated in the September 11th attacks of 2001, a sorrowful event starkly exhibiting the worst of humankind. The ramp-up of anti-terrorist initiatives by multiple nation states in reaction to the 9/11 attacks, although preventing another disaster of such proportions, has generally been ineffectual in curbing the spread and influence of terrorism. Terrorism still runs rampant across the world, with powerful groups such as Boko Haram, FARC, and ISIS wielding sizable power in their respective regions. Although it is easy to associate terrorism with large, theatrical events in the Western world such as 9/11, the millions of individuals that have been killed or abused under local terrorist regimes must be placed into consideration as well.

The success of terrorism thus far rests heavily upon the ability of terrorists to adapt - in particular, adopting modern technologies to achieve their objectives. In one sense, this can be observed by the use of destructive weaponry and high-tech equipment when engaging in terroristic activities or combating peacekeeping forces. However, a more discreet, but equally potent force that forms the foundation for much terrorism can be found in the digital sphere. Terrorists frequently rely on online platforms to advertise their cause, communicate with one another, and finance their projects. Since the Internet and digital media are very much still in their infancy, terrorists have discovered numerous opportunities in exploiting the deficiencies of online security, slipping around the established physical barriers upholding public security and adding a new dimension to their danger. As such, it is imperative that discussion on cybersecurity be undertaken when considering the question of terrorism.

Definition of Key Terms

Terrorism

Since 1994, the United Nations has commonly used the following description to condemn terrorist acts: "Criminal acts intended or calculated to provoke a state of terror in the public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.”

Social Media

Computer-based technologies that facilitate the sharing of ideas, thoughts, and information through the building of virtual networks and communities.

Cybersecurity

The protection of computer systems and networks from criminal use of electronic data.

Information and Communication Technology (ICT)

The use of computers and other electronic equipment and systems to collect, store, use, and send data electronically

Cryptocurrency

A form of currency that only exists digitally which usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units. Cryptocurrencies rely on cryptography to prevent counterfeiting and fraudulent transactions.

Online Infrastructure

The fundamental facilities and systems connected to or under computer control that serve a country, city, or other area, including the services and facilities necessary for its economy to function.

History & Developments

A Brief Timeline of Terrorism

Origins and Development of Terrorism

The reign of terror instituted by statesman Maximilien Robespierre following the French Revolution formed the basis of modern terrorism - using unlawful and violent means to achieve political goals. However, by the 1950s, terrorism had become more associated with attacks against an established order rather than state-led oppression. During this period, the boom of ethnic nationalism and anti-colonial sentiment, coupled with regional poverty and the introduction of international borders, gave rise to non-state actors employing guerrilla style tactics in search of power and/or autonomy. Examples of these groups include the Irish Republican Army, the Kurdish Worker’s Party, and the Sri Lankan Liberation Tigers, all of whom utilized destructive tactics (often against civilians) in attempt to create independent states. Terrorism rose to international prominence by the late 60s, when terrorists began turning their sights to foreign targets, often far across the globe, as a symbolic showcase of power. Hijackings, bombings, and even disruptions to major international events (Black September and the 1972 Olympics being a prime example) brought fear to citizens around the globe, and attached an element of the spectacular in the public’s perception on terrorism. These developments also coincided with the growing availability of military grade weaponry in black market trade, meaning that many terrorists organizations began accumulating substantial authority on both the local and international stage. By this stage, counterterrorism had become a topic of frequent discussion by nation states, but little international consensus could be achieved on defining terrorism or creating a unified plan in opposing such groups.

Terrorism in the 21st Century

With the dawn of the twenty-first century also came the alarming ascent of religious terrorism, which is widely perceived as the most destructive and influential form of terrorism today. Combining religious zeal with brutal violence, groups such as Al Qaeda, Hamas, and Hezbollah have attracted thousands of disciples, most of which are young men. Although the stereotypical extremist group is Islamic, other faiths from Judaism to Hinduism also have their own forms of religious terrorists. For instance, the Jewish Underground was a right wing extremist group which committed a series of violent anti-Arab crimes against Palestinians in the 1980s, most notably with the infamous 1984 plot to blow up the Dome of the Rock. The scope of terrorism’s (especially in the religious sense) international expansion was made clear on September 11th, 2001, when over 3,000 individuals perished as Al-Qaeda launched a series of coordinated assaults on American soil. Panic reverberated around the globe and countries rapidly expanded their antiterrorist programs. The United States spent trillions of dollars on the controversial “War on Terror”, which targeted fundamentalist Sunni armed groups throughout the Muslim world. Unfortunately, while research suggests that countries not suffering from civil conflict were less likely to experience terrorism after the events of 9/11, Muslim-heavy regions suffered from more domestic terrorism as the international community cracked down on terrorism. This shows that foreign intervention in regions such as Afghanistan and Iraq have failed to restore order, instead destabilizing local societies and thereby bolstering the fundamentalist drive of terrorists. As of recent times, according to the Global Terrorism Index, the total number of deaths resulting from terrorism has decreased by 53% to 15,952 from the peak of 2014 to 2018. However, it must be kept in mind that these present only the recorded number of deaths, and terrorist activities encompass far more than just the murder of individuals. Relatively young organizations, such as the Khorasan Chapter and Al-Shabaab, along with established extremist groups such as the Taliban and Boko Haram, are still at large and abusing the human rights of thousands.

Digital Terrorism

Threats of Digital Terrorism

With the advent of the digital age, terrorists have also sought to exploit the mechanisms of the online world. Member states of the United Nations have frequently expressed concern at the use of ICT by terrorists to commit, recruit for, and fund terrorist activities. Indeed, with the modern world so dependent on digital technologies, terrorists are able to cause significant infrastructural damage by directing attacks on critical control systems. It is conceivable that energy, water-supply and transportation systems can suffer enormous damage at the hands of hackers and cyber terrorists, especially with worrying evidence that ISIL and other terrorist groups are recruiting professionals capable of such feats. As technology invariably continues developing, the opportunity for abusing it also increases. With new fields like artificial intelligence and big data undergoing breakthrough after breakthrough, it is dispiriting to imagine such powerful tools at the disposal of terrorists, and that the threats that they will pose to personal privacy, security and overall well-being. Recent discussions in the UN over “killer robots”, or unmanned drones, tanks, warships, and artillery guns, have sparked concern over terrorist access to these weapons. Prominent experts in the field of AI weaponry such as engineer Alvin Wilby and professor Noel Sharkey have all addressed various governments on the threat of lethal artificial intelligence in terrorist hands.

Terrorist Content in the Digital Sphere

Furthermore, terrorist groups have embraced social media as a means of advertisement and self-glorification. The Islamic State holds thousands of accounts across Twitter, Instagram, and Youtube, which constantly spouts propaganda and documentation of their activities. For an extreme case, approximately 40,000 tweets were posted in a single day the extremist group’s forces launched an offensive in the city of Mosul, Iraq. These messages are incredibly effective in convincing people of the organization’s strength and piety, luring (mostly) young men into its depths with a tantalizing offer of religious self-actualization. The macabre 2019 livestream of far-right extremist Brenton Tarrant massacring praying Muslims in Christchurch demonstrates the dangers social media poses in propagating terrorist content, especially considering the wide viewership the broadcast attracted. A cheaper and more efficient method of communication, terrorists rely heavily on online platforms for recruitment and training procedures, as well as keeping in touch with donors. Youth are especially vulnerable to terrorist exploitation, whether through physical and cultural threats or false promises of economic security, self-worth, and religious glory. Much of this content is transmitted online through extremist websites, propaganda on digital public spheres, or even personal messaging, allowing terrorists to connect with a larger number of young individuals. Although social media companies and governments have attempted to censor terrorist content online, the sheer volume of material posted makes it difficult to block the flow of this dangerous information. Even worse, Al-Qaeda has been known to use social media platforms and the Internet to plan operations, distribute material discretely, and communicate with one another. Terrorists are also drawn to the general lack of regulatory oversight on cryptocurrencies, allowing them to carry out numerous illicit transactions with online mediums of exchange. Regulations in the United States, Europe, and China makes it difficult to obtain bitcoin anonymously on an exchange. However, if trading occurs on a decentralized exchange or in a country without proper regulation, the transactions could become much harder to trace.

Geopolitics

United Nations Counter Terrorism Center (UNCCT)

The UNCCT is an official branch of the UN focused solely on countering terrorism on global, regional, and national levels. Its current advisory board consists of 21 member states along with the European Union, and is chaired by Saudi Arabia. A full list of member states follows: Saudi Arabia (Chair), Algeria, Argentina, Belgium, Brazil, China, Egypt, European Union, France, Germany, India, Indonesia, Morocco, Nigeria, Norway, Russian Federation, Pakistan, Spain, Switzerland, Turkey, United Kingdom, and United States of America.

United States

The United States has historically led the globe in counterterrorist initiatives. The country has spent trillions of dollars waging war with terrorists across the Middle East, oftentimes infuriating local governments with the scale of their intervention. In reaction to the 9/11 attacks, President Bush along with a coalition of Western powers launched a full-scale assault on the Afghan Taliban government, soon followed by an invasion of Iraq in 2003 following intelligence that dictator Saddam Hussein possessed weapons of mass destruction. In tactical terms, some successes of this “war” can be seen in the killing of hundreds of terrorist leaders and overall spread of awareness on terrorism. However, overall terrorist influence in areas of intervention by the United States has failed to decrease dramatically, while continuous warfare has brought devastation to local populations. It is arguable that the ineffectiveness of this confrontational approach should be replaced by measures to uplift social, political, and economical conditions in areas plagued by terrorism, but Washington continues to pour billions into military and security forces abroad. Despite these shortcomings, the United States actively pursues solutions to countering digital terrorism, and openly cooperates with other member nations and independent businesses alike on this issue. It must be kept in mind that rights such as personal privacy are heavily prioritized when discussing methods of online surveillance.

Afghanistan

Since the early 1980s, Afghanistan has been plagued by continuous conflict and instability. A Soviet invasion of the nation in 1979 incited a wave of backlash from Islamic fighters, eventually collapsing the new Marxist regime a decade later. Civil war broke out as this power vacuum emerged, and the Taliban quickly overran over 90 percent of Afghan territory with the help of al-Qaeda. Further conflict followed in the wake of 9/11, when US and coalition forces eradicated Taliban presence in the region. Although the invasion proved to be devastatingly effective, the ensuing nation-building efforts were doomed by a lack of funding, inadequate planning, and rampant corruption within Afghan government. Widespread anti-Western sentiment among Afghans over the slow pace of reconstruction, the weakness of the new democratic government, and the treatment of Afghan citizens by US and NATO forces culminated in the resurgence of the Taliban ongoing since 2005.

Currently, the situation in Afghanistan has entered a stalemate after 18 years of war, with the country divided between the official government (recognized internationally), the Taliban, the Islamic State, and a handful of smaller terrorist organizations. The Afghan government currently controls the capital Kabul and around 30% of the region. It partners with the US and NATO in antiterrorist initiatives, and continues to engage in combat with various terrorist groups. However, the Taliban is a steadily growing force in the nation, currently holding more territory than in any other time since initial US invasions in 2001. It has been a unifying force for lesser terrorist organization, with online advertising playing a crucial role in its revival.

***Figure 1: Taliban Control in Afghanistan***

Iraq

Similar to the situation in Afghanistan, foreign intervention in the 21st century has brought chaos to Iraq. Over accusations on the possession of nuclear weapons, the US deployed its forces across the nation in 2003 and ended the oppressive rule of dictator Saddam Hussein. However, turmoil erupted as the Hussein regime collapsed, with a full-scale civil war compounding further misery onto a country which had already faced decades of economic mismanagement and ruthless oppression. The Iraq War also created the direct successor of Al-Qaeda, the Islamic State (known as ISIL, ISIS, or IS). The organization evolved from a Sunni insurgency against the Iraqi government and foreign forces, and seized the opportunity of the Syrian Civil War to establish authority across Syria’s eastern territories. It then pushed on to gain more land in Iraq and Syria, claiming a caliphate over ISIS controlled soil in 2014. The organization relies on brutal tactics, which it often broadcasts as propaganda, as a central force in maintaining its reign of terror.

ISIS remains a serious force in Iraq today, destabilizing the local government through a violent campaign and terrorizing citizens throughout the region. The Iraqi government is a key member of the Global Coalition to Defeat ISIS and also contributes to international organizations involved in activities such as repelling foreign terrorist fighters, stabilizing threatened communities and facilitating communications.

Boko Haram

Boko Haram is a Nigerian Islamic extremist group aiming to oppose Western influence and impose Islamic law. Initially formed as a response to the corruption and economic disparity present in Nigeria, the group embarked upon a campaign of vengeance in 2009 after a series of police-initiated attacks left several hundred members of Boko Haram including their leader dead. They directed numerous coordinated assaults against the government, Christian Churches, and schools, gaining control over large sections of rural Nigeria. In 2015, the group pledged allegiance to ISIL, and has continued to disregard human rights and confront organized authority since then. The shadowy nature of Boko Haram’s operations makes it difficult to eradicate, while the civilian casualties resulting from an ongoing war between the group and the Nigerian government raises severe international concern.

Previous Attempts to Solve the Issue

Cybersecurity and digital terrorism have been regularly discussed in the UN since the early 2000s. The UN Security Council emphasizes the significance of digital technology in counterterrorism, with Resolution 1373 calling on member states to increase the exchange of information on the use of ICT by terrorist groups, and Resolution 2129 acknowledging the growing connection between terrorism and ICT. Especially through work done by the UNCCT, as well as aligning counterterrorist objectives with combatting other forms of organized digital crime, some progress has been made on restricting terrorist activities in the online domain. For example, facilities for collecting digital evidence against cybercrime have steadily evolved, with many states becoming more willing to participate in international data sharing to track and prosecute perpetrators of terrorist crimes. Programs such as Legal Access to Digital Data Across Borders have greatly enhanced the ability of authorities and investigators to obtain online evidence and cooperate with private corporations to protect human rights. Tech Against Terrorism is another UN initiative which advocates for stronger self-regulation within the private sector to prevent terrorists from abusing existing technologies. It currently works with major companies such as Microsoft and Facebook to research technological methods of restricting the impact of terrorists online. These measures should prove to be a useful foundation for future counterterrorist framework, but much development is needed to create a comprehensive shield against terrorist content. Perhaps with facilitation from the UN, more cooperation could be achieved between separate agencies.

On the national level, many nation states are investing in offensive and defensive ICT capabilities useful in countering malignant digital forces. These include reconnaissance, information operations and network disruption services. However, trust needs to be established between nation states such that use of this technology on the international stage against terrorists is authorized and beneficial technology is shared. Many effective technologies that could contribute to stemming digital terrorism are not put to use in heavily afflicted regions, due to an unwillingness to share ICT technology or restrictions on local online security systems. Currently, foundations such as the Organization for Security and Cooperation in Europe (OSCE) are holding confidence-building conferences to secure the cyberspace and encourage online partnership between states.

In 2015, the UN held a special meeting in the hopes of stemming the flow of foreign terrorist fighters (FTFs). Here, the Madrid Guiding Principles were born, a practical tool for member states to follow on combatting terrorism. Amongst the guidelines, guiding principles 25 and 26 specifically recommend measures involving ICT and data collection when dealing with digital terrorism. The former suggests electronic surveillance implemented in cases related to FTFs, while the latter calls for competent ICT and forensic capacities to be installed in national law-enforcement agencies, all of which should respect international human rights laws including freedom of expression. The International Criminal Police Organization (INTERPOL) has been analyzing terrorist use of social media platforms to bolster identification and detection efforts for years now. Through collecting electronic records, gathering e-evidence internationally, and engaging with the private sector to work with law-enforcement agencies, INTERPOL provides a practical platform on which future models for online security can be built upon. The next step is to encourage adherence to existing policies, and developing incentives to do so through education on the benefits of counterterrorism and economic bonuses.

Recently, the UNCCT launched its global cybersecurity program aimed at delivering awareness raising workshops to member states. Phase 1 was launched in South East Asia last year, with 11 member states participating in these tailored workshops. Regions of the Horn of Africa, East Africa, and the Sahel will also receive access to such initiatives soon.

Relevant UN Treaties and Events

* 6th review of the UN Global Counter-Terrorism Strategy A/RES/72/284
* UN Security Council Resolution 2341 (2017)
* UN Security Council Resolution 2370 (2017)
* Security Council text S/2015/939 (Madrid Guiding Principles)
* UN Security Council Resolution 1373 (2001)
* UN Security Council Resolution 2129 (2013)

Possible Solutions

First, delegates may find it useful to **devise a complete definition regarding terrorism**. The major obstacle blockading UN officials from achieving this seemingly simple task is that terrorism is difficult to distinguish from other forms of political violence and crime. It needs to be agreed on whether terrorism is limited to attacks on civilians or extended to include governmental forces such as the military, and if abusive regimes can be considered as terrorist. In addition, varying perceptions of “good and bad” in the international community means that it is almost impossible to officially label an organization as terrorist in UN without inciting a great deal of outrage. As the old adage goes, “one man’s freedom fighter is another man’s terrorist”. Although the challenges of creating a universal definition are enormous, a full definition can help with streamlining solutions to match the criteria of activities deemed as terrorist.

A major question concerning the question of digital terrorism involves human rights and privacy. It is undeniable that **a certain level of surveillance is necessary in detecting terrorist threats online**. However, when public safety will have to compromise online privacy is a question that countries view in various ways. Optimally, data collection should circumnavigate large parts of the population unaffiliated with terrorists and concentrate on key elements that are identified as terroristic. Even if such regulatory measures already exist in many countries, UN governance over these structures would safeguard the human rights of all citizens involved, and could push nations with insufficient or dysfunctional cybersecurity systems to reach set international standards (yet to be created). The establishment of an enforced set of international search parameters should prove to be considerable progress in negating the elusiveness of terrorism online while maintaining humanitarian standards. Maintaining communications with victims of terrorism will assist locating the presence of terrorists online, as with training local police forces in identifying digital terrorism. Developing websites dedicated to educating youth on the threat of terrorism may also nullify a part of terrorist recruitment online, and bolster the reporting of terroristic content online to relevant authorities. In addition, new technologies such as AI will be invaluable in the near future to process large amounts of information and identifying potentially dangerous material. Facebook already utilizes image matching technology and machine learning algorithms to detect terrorist propaganda, which has been successful to a certain degree. All in all, the problem is not that we lack the resources or technological capability to track down instances of digital terrorist activity. It is more about how these resources are used, and in what ways they can be used in an appropriate and ethical manner.

Delegates must also seek to **install regulatory mechanisms throughout online facilities** to avoid terrorist misuse. As most online infrastructure, social media platforms, cryptocurrencies that terrorists target are designed and operated by non-terrorists, it is critical to communicate with private or government agencies for the sake of securing these domains. For example, rigorous cybersecurity measures could be mandated by local governments, social media platforms could be held legally accountable for the spread of terrorist content, and cryptocurrencies could be regulated by international and local police just as traditional banks are. The UN needs to encourage local governments to prosecute and impose severe punishments on corporations spreading terrorist content willingly. Even platforms unknowingly propagating terrorist material should face some consequences for the lack of basic security. An international panel assisting governments to judge the criminality of activities online or suitable repercussions for corporations can further promote accountability. Currently, as we are just beginning to recognize the power that these technologies hold, there is a woeful neglect of boundaries placed on the gadgets at our disposal.

Finally, **unifying the global campaign against terrorism** is necessary to guarantee the feasibility and efficiency of any action taken. There exists hundreds of countries, thousands of organizations, and millions of dedicated individuals seeking to end the looming threat of terrorism, but for the most part they are separated, working with different agendas and methods. Perhaps by abandoning this scattergun approach, and organizing a combination of these bodies into one, cohesive entity, decisions can be made faster, radical plans can be executed, and more cooperation can be achieved. It all comes down to establishing clear, common objectives that the majority of nation states can agree to.

Bibliography

"Analysing social media." *INTERPOL*, 2020, [www.interpol.int/Crimes/Terrorism/Analysing-social-media](http://www.interpol.int/Crimes/Terrorism/Analysing-social-media).

"A Timeline of the U.S.- Led War on Terror." *History*, 5 May 2020, [www.history.com/topics/21st-century/](http://www.history.com/topics/21st-century/) war-on-terror-timeline.

Bezhan, Frud. "The Taliban, The Government, And Islamic State: Who Controls What In Afghanistan?" *Radio Liberty*, 31 May 2020, [www.rferl.org/a/taliban-government-islamic-state-who-](http://www.rferl.org/a/taliban-government-islamic-state-who-) controls-what-in-afghanistan-/30644646.html.

Coninsx, Michele. "Responding to terrorist use of the internet." *Global Initiative*, 21 Jan. 2019, [globalinitiative.net/terrorist\_use\_internet/](http://globalinitiative.net/terrorist_use_internet/).

"Cyber/ICT Security." *OSCE*, 2020, [www.osce.org/cyber-ict-security](http://www.osce.org/cyber-ict-security).

Dion-Schwarz, Cynthia, et al. "Terrorist Use of Cryptocurrencies." *RAND Corporation*, 2019, [www.rand.org/pubs/research\_reports/RR3026.html](http://www.rand.org/pubs/research_reports/RR3026.html).

Encyclopedia Britannica Editors. "Iraq War." *Encyclopedia Britannica*, 29 Nov. 2019, [www.britannica.com/event/Iraq-War](http://www.britannica.com/event/Iraq-War).

Larkin, Sean. "Why Can’t We Agree on a Definition of Terrorism?" *Open Mind*, 16 Dec. 2013, [www.bbvaopenmind.com/en/economy/geopolitics/why-cant-we-agree-on-a-definition-of-terrorism/](http://www.bbvaopenmind.com/en/economy/geopolitics/why-cant-we-agree-on-a-definition-of-terrorism/).

Marr, Bernard. "Weaponizing Artificial Intelligence: The Scary Prospect Of AI-Enabled Terrorism." *Bernard Marr & Co.*, 2020, [bernardmarr.com/default.asp?contentID=1421](http://bernardmarr.com/default.asp?contentID=1421).

Ritchie, Hannah, et al. "Terrorism." *Our World in Data*, July 2019, ourworldindata.org/terrorism.

Smith, Meagan, and Sean M. Zeigler. "Terrorism before and after 9/11 â a more dangerous world?" *Sage Journals*, 10 Nov. 2017, [journals.sagepub.com/doi/full/10.1177/2053168017739757](http://journals.sagepub.com/doi/full/10.1177/2053168017739757).

Tech Against Terrorism. "Tech Against Terrorism." July 2020, [www.techagainstterrorism.org](http://www.techagainstterrorism.org).

UN. "Cybersecurity." *Office of Counter-Terrorism*, [www.un.org/counterterrorism/cybersecurity](http://www.un.org/counterterrorism/cybersecurity).

UN. "Madrid Guiding Principles." *UN*, 23 Dec. 2015, [www.un.org/sc/ctc/wp-content/uploads/2016/10/Madrid-Guiding-Principles\_EN.pdf](http://www.un.org/sc/ctc/wp-content/uploads/2016/10/Madrid-Guiding-Principles_EN.pdf).

UN. "Terrorism Financing." *Security Council Counter-Terrorism Committee*, [www.un.org/sc/ctc/focus-areas/financing-of-terrorism/](http://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/).

UN. "Youth Engagement." *Office of Counter-Terrorism*, [www.un.org/counterterrorism/youth-engagement](http://www.un.org/counterterrorism/youth-engagement).

Witte, Griff. "Afghanistan War." *Encyclopedia Britannica*, 5 Mar. 2020, [www.britannica.com/event/Afghanistan-War](http://www.britannica.com/event/Afghanistan-War).