30th Annual

BRIGHAM YOUNG UNIVERSITY MODEL UNITED NATIONS CONFERENCE

Sponsored by the David M. Kennedy Center for International Studies
Friday, November 8th, 2019 – Provo, Utah

Dear Delegates,

Welcome to the 30th annual Brigham Young University Model United Nations Conference (BYUMUN). My name is Gracia Lee, and I will be serving as your Director for the Security Council. I am a sophomore majoring in Graphic Design and minoring in Tagalog here at BYU, but I spent the summer studying Hawaiian culture and Polynesian art at BYU-Hawaii. Last year, I represented Turkmenistan on the General Assembly Second Committee for BYU at the National Model United Nations Conference (NMUN). I've been involved in high school MUN programs for over five years, and it's been one of the most valuable parts of my education. I am excited to work with each of you at this year's conference!

This year, the topics before the Security Council are:

I. Addressing Cybersecurity in Elections and Infrastructure Sabotage
II. Combating the Financing of Terrorism through Non-Profit Organizations.

The chief duty of the Security Council is to hold accountable those who are responsible for condemnable actions, and simultaneously minimize the impact these measures have on innocent parts of the population and economy.

This Background Guide will serve as a resource to springboard your research, but it's not intended to replace it. I hope and expect that you will study these topics in depth and come prepared to share innovative solutions to these problems. The more knowledgeable you are in discussing these topics, the more effective you can be as a delegate.

Delegates, I wish you the best of luck as you prepare. Please contact me with any questions or concerns!

Gracia Lee
Director, Security Council
gracia@plainsimple.org

BYUMUN – 120 HRCB – Provo, UT 84602
801.422.6921 – byumun@byu.edu
http://byumun.byu.edu

Committee History

"The United Nations remains our most important global actor. These days we are continuously reminded of the enormous responsibility of the Security Council to uphold international peace and stability."
— Anna Lindh, Swedish Minister for Foreign Affairs (1998-2003)

Introduction

Following the devastating effects of the two world wars, the international community created the United Nations (UN) and its six subsidiary bodies. The Charter of the United Nations was signed in 1945, and Articles 23-32 created the Security Council to address issues of global peace and security.[1] Article 23 established five permanent members of the Security Council: China, France, the Soviet Union (now the Russian Federation), the United Kingdom of Great Britain and Northern Ireland, and the United States of America. These five countries, often referred to as the "P5," have the power to veto any substantive resolution. In addition to these permanent seats, there are also ten rotating seats who are elected on a regional basis to serve for a period of two years. Article 25 of the UN Charter says that "The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter".[2] This means that the Security Council is the only body in the United Nations that can make decisions that are legally binding on all Member States, and if necessary, they enforce their resolutions with measures such as embargoes, sanctions, and even military action. However, if the Council cannot reach a passing vote (at least nine votes without a veto), they may choose to simply apply political pressure by producing a non-binding presidential statement instead.

Successes and Failures

The Security Council's primary purpose is to tackle threats to global peace and safety. And on a macro scale, they seem to have achieved this: Canadian psychologist and Harvard University professor Stephen Pinker says that we are living in the most peaceful time in human history, and the Council on Foreign Relations (CFR) says this can be attributed to the work of the Security Council.[3] Since its founding, the Security Council has an impressive record of resolving international conflicts. One example of this is the signing of the peace agreement between the Government of Colombia and the Revolutionary Armed Forces in November 2016, which marked the end of the Western Hemisphere's longest-running conflict.[4] In January 2016, the Security Council unanimously adopted resolution A/RES/2261, which supported the ongoing peace talks in Havana, Cuba, and included the decision to moderate the end of the conflict in Colombia. This is one of only fourteen decisions the Security Council has adopted unanimously in its history. Later in November 2016, the final peace agreement that had been moderated by the Security Council was ratified in the Columbian Congress. After the implicit invitation of the

[1] "U.N. Charter (Full Text)." United Nations. Accessed June 11, 2019. https://www.un.org/en/sections/un-charter/un-charter-full-text/.
[2] Ibid.
[3] Pinker, Steven. The Better Angels of Our Nature: Why Violence Has Declined. NY, NY: Penguin Books, 2012: 252-254.
[4] "Final Agreement for Ending the Conflict and Building a Stable and Lasting Peace." United Nations. April 21, 2017. Accessed June 29, 2019. https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2017/272.

conflict parties in Section 6.3 of the final agreement, the United Nations currently monitors compliance with the final peace agreement.[5]

Other accomplishments of the Security Council include UN peacekeeping efforts. Since 1945, UN peacekeepers have undertaken over 60 field missions and negotiated 172 peaceful settlements; some of the most notable being in Cambodia, El Salvador, Guatemala, Mozambique, Namibia, and Tajikistan.[6] Peacekeeping missions are the most visible face of the Security Council's conflict-management work; currently, the Council is overseeing fourteen global operations (involving roughly ninety thousand uniformed personnel) that are protecting millions of people all over the world.[7] These operations are monitored by the General Assembly Fourth Committee (GA4), who reviews all issues regarding peacekeeping and considers new proposals to enhance peacekeeper's abilities to fulfil their responsibilities.[8] Some of these current efforts include missions to the Central African Republic, Mali, the Democratic Republic of the Congo, and South Sudan. Peacekeeping efforts include the protection of civilians, human rights monitoring, the implementation of transnational roadmaps, and the support for the delivery of humanitarian assistance in corrupted areas.

However, the Security Council has had many shortcomings and even outright failures. Two of the most glaring examples are the lack of action during the genocides in Rwanda (1994) and Darfur (2003 - ongoing), which indirectly and directly killed over 1.5 million people combined, displacing millions more.[9] This was a result of a systemic failure within the United Nations to address the reports of crises in the areas, and the ineffectiveness of the peacekeeping mission's mandates. For example, peacekeeping forces in Rwanda had a mandate that prevented them from taking military action, which proved catastrophic after the government launched the slaughter of an estimated 800,000 ethnic minority Tutsis and Hutus in 1994. The peacekeeping forces stationed in Rwanda were unable to protect civilians due to their flawed mandate. After rampaging killers killed ten Belgian peacekeepers at the beginning of the genocide, there was little will to keep the peacekeepers in place, much less to strengthen their mandate. Peacekeeping forces abandoned a school where civilians had massed in hopes of protection, which led to a schoolyard massacre of thousands of people.

The Security Council has also faced steep structural criticisms in recent years. One notable source of contention is the number of members (both permanent and non-permanent) on the Security Council. Critics argue that the modern Security Council has failed to adapt to the geopolitical realities of the twenty-first century; with U.N. Member States such as Brazil,

[5] Ibid.

[6] "Our Successes Peacekeeping." United Nations. Accessed June 11, 2019. https://peacekeeping.un.org/en/our-successes.

[7] "Where We Operate Peacekeeping." United Nations. Accessed June 11, 2019. https://peacekeeping.un.org/en/where-we-operate.

[8] "Report of the Special Committee on Peacekeeping Operations." United Nations. March 09, 2018. Accessed August 06, 2019. https://www.un.org/ga/search/view_doc.asp?symbol=A/72/19.

[9] "Report of the Independent Inquiry into the Actions of the United Nations during the 1994 Genocide in Rwanda." Security Council Report. December 15, 1999. Accessed June 11, 2019. http://www.securitycouncilreport.org/atf/cf/{65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9}/POC S19991257.pdf; "Death Toll in Sudan's War-torn Darfur Region up to 70,000 - UN Health Agency | UN News." United Nations. October 18, 2004. Accessed June 11, 2019. https://news.un.org/en/story/2004/10/118252-death-toll-sudans-war-torn-darfur-region-70000-un-health-agency.

Germany, Japan, India, Nigeria, and South Africa calling for expansion and pressing for their own permanent seats.[10] They say that the Security Council has become undemocratic and outdated, with the P5 countries failing to adequately represent regions such as South America, Oceania, Southern Asia, Africa, and the Middle East. In their words, this lack of representation has led to a systemic failure within the Security Council to protect the under-represented regions of the world.[11]

Mandate

The primary duty of the Security Council is to maintain international peace and security in accordance with the principles and purposes of the United Nations.[12] To do this, it focuses on fostering international cooperation and developing bilateral relationships between Member States, with an emphasis on promoting the protection of human rights. Additionally, it appoints judges to the International Court of Justice.[13]

When there is a threat to global safety, the Security Council's first mode of action is to recommend that the parties try to reach an agreement by peaceful means. This can be manifested in the forms of mediation, peacekeeping missions, investigations, and setting forth standards for compromise.[14] If this fails and the situation becomes hostile, the Council will issue ceasefire directives, dispatch peacekeeping forces to separate members of the conflict, impart sanctions or embargoes, or even take collective military action.[15] As mentioned above in regards to the Rwandan genocide, it's often difficult for non-coercive efforts to have much effect in times of extreme crisis. However, if the Security Council is able to address issues before they escalate to the devastating scales of the Darfur and Rwandan genocides, these measures can be very effective in preventing violent armed conflict.

Conclusion

The Security Council, despite its failures, flaws, and shortcomings, has prevented and mitigated atrocities committed during times of conflict. Members of the Security Council, both permanent and non-permanent members, must continue to work together to foster international cooperation and implement necessary changes. The uniquely impactful mandate of the Security Council must be utilized to set international norms and govern state actions.

[10] Runjic, Ljubo. "Reform of the United Nations Security Council: The Emperor Has No Clothes." Revista De Direito Internacional 14, no. 2 (2017). doi:10.5102/rdi.v14i2.4587.
[11] Ibid.
[12] "Functions and Powers of the Security Council." United Nations. Accessed June 11, 2019. https://www.un.org/securitycouncil/content/functions-and-powers.
[13] Ibid.
[14] "What Is the Security Council? Security Council." United Nations. Accessed June 11, 2019. https://www.un.org/securitycouncil/content/what-security-council.
[15] Ibid.

Annotated Bibliography

"Death Toll in Sudan's War-torn Darfur Region up to 70,000 - UN Health Agency | UN News." United Nations. October 18, 2004. Accessed June 11, 2019. https://news.un.org/en/story/2004/10/118252-death-toll-sudans-war-torn-darfur-region-70000-un-health-agency.

> *This press release summarizes a report released by the World Health Organization (WHO), which details the number of civilians affected by the Darfur genocide both directly and indirectly.*

"Final Agreement for Ending the Conflict and Building a Stable and Lasting Peace." United Nations. April 21, 2017. Accessed June 29, 2019. https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2017/272.

> *This resolution details the peace agreement between the Columbian government and communist guerillas, which ended decades of armed conflict. The agreement was reached under the oversight of the Security Council.*

"Functions and Powers of the Security Council." United Nations. Accessed June 11, 2019. https://www.un.org/securitycouncil/content/functions-and-powers.

> *This source provides information on the Security Council's powers, functions, duties, and mandate.*

"Our Successes Peacekeeping." United Nations. Accessed June 11, 2019. https://peacekeeping.un.org/en/our-successes.

> *This source discusses the past successes of the U.N. Peacekeeping forces and the factors required for a successful peacekeeping mission.*

Pinker, Steven. *The Better Angels of Our Nature: Why Violence Has Declined*. NY, NY: Penguin Books, 2011: 252-254.

> *In this book, the author argues that violence in the world has declined both in the long run and in the short run and suggests explanations as to why this has occurred.*

"Report of the Independent Inquiry into the Actions of the United Nations during the 1994 Genocide in Rwanda." Security Council Report. December 15, 1999. Accessed June 11, 2019. http://www.securitycouncilreport.org/atf/cf/{65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9}/POC S19991257.pdf.

> *This report explores the actions of the U.N. during the Rwandan genocide and goes into detail about the number of civilians affected both indirectly and directly by their lack of action.*

"Report of the Special Committee on Peacekeeping Operations." United Nations. March 09, 2018. Accessed August 06, 2019. https://www.un.org/ga/search/view_doc.asp?symbol=A/72/19.

This report details the GA4's review of the Security Council's peacekeeping operations throughout 2017 and 2018.

Runjic, Ljubo. "Reform of the United Nations Security Council: The Emperor Has No Clothes." ***Revista De Direito Internacional*** **14, no. 2 (2017). doi:10.5102/rdi.v14i2.4587.**

This journal discusses proposed methods of Security Council reform and the claims to permanent Council seats from individual countries.

"United Nations Charter (Full Text)." United Nations. Accessed June 11, 2019. https://www.un.org/en/sections/un-charter/un-charter-full-text/.

The U.N. Charter is the foundational treaty for the creation of the United Nations.

"What is the Security Council? Security Council." United Nations. Accessed June 11, 2019. https://www.un.org/securitycouncil/content/what-security-council.

This article introduces the Security Council and outlines possible methods for action against threats to global peace and security.

"Where We Operate Peacekeeping." United Nations. Accessed June 11, 2019. https://peacekeeping.un.org/en/where-we-operate.

This source shows where all current Peacekeeping operations are, and includes fact mission sheets for each ongoing mission.

I. Addressing Cybersecurity in Elections and Infrastructure Sabotage

"We have agreed that cybersecurity is a global issue that can only be solved through global partnership. It affects all organizations, and the United Nations is positioned to bring its strategic and analytic capabilities to address these issues."
— His Excellency Mr. Lazarous Kapambwe, President of ECOSOC (2011)

Introduction

Dependence on the internet is rapidly increasing on a worldwide scale. With this, the prominence of cybersecurity issues has also risen; causing many national and regional governments to adopt policies that reflect international "cyber norms" that have been suggested by bodies such as the United Nations General Assembly (UNGA).[16] However, UN action has been relatively sluggish in creating binding policy concerning cybercrime. This is primarily because the Security Council, the only UN organ with binding power, has not been involved in the discussion until the last few years. This is continually proving to be a threat to international security, and the Security Council must take charge and quickly address these cyber challenges by affirming and clarifying the application of international law to state behavior in the cyberspace.

As of 2019, the UN only has one agency that specializes in cyber threats, the International Telecommunications Union (ITU). In their 2017 Global Cybersecurity Index (GCI), the ITU reported that only 38 percent of countries have a published cybersecurity strategy and an additional 12 percent of governments are in the process of developing one. This leaves 50 percent of the world's countries virtually unprotected to digital attacks. The report reads: "Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective. [Cybersecurity is] becoming more and more relevant in the minds of countries' decision makers."[17]

One of the primary responsibilities of the Security Council will be creating cohesive definitions of new terms such as "cyberterrorism" and "cyberwarfare." Theresa Payton, an expert in the field of cybersecurity and former United States White House chief information officer, said: "We haven't actually defined what is considered an act of war in the cybersecurity realm. We have in the physical realm: if tanks move in certain directions, if missiles are fired, if airplanes are in the wrong airspace, [or] if ships are in the wrong shipping lanes. But we haven't done that for the digital space."[18] The creation of these definitions is a crucial aspect of maintaining continuity in the international community, assisting Member States in identifying cyberattacks, and creating precedence for proportioned responses.

[16] Henderson, Christian. "The United Nations and the Regulation of Cybersecurity." Research Handbook on International Law and Cyberspace, 2015. Accessed July 1, 2019. https://www.elgaronline.com/view/9781782547389.00035.xml.

[17] "Global Cybersecurity Index (GCI) 2017." International Telecommunications Union, 2017. Accessed July 2, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[18] Stewart, Emily. ""This Is Now the New Normal": An Expert Explains Why Cybersecurity Risks Aren't Going Away." Vox. August 26, 2018. Accessed July 04, 2019. https://www.vox.com/policy-and-politics/2018/8/26/17782408/russia-iran-cybersecurity-threat-facebook-midterms.

Additionally, special attention must be paid to the protection of election security infrastructure. Article 21 of the Universal Declaration of Human Rights states: "The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which ...shall be held by secret vote or by equivalent free voting procedures."[19] Election security is a critical aspect of this democratic process, fundamental to public engagement and, by extension, integral to the goal of an election itself.

Protecting Critical Infrastructure

While all cyberattacks must be regarded as threatening, certain infrastructures are critical to national security and stability. If successfully attacked, these can severely cripple a nation. A few of these critical infrastructures are election security, energy resources, finance systems, telecommunications, transportation, and water systems.[20] One of the first known attacks on critical infrastructure was the late-2000s Operation Olympic Games, a covert cyberattack by the United States and Israel directed at Iranian nuclear facilities.[21] This temporarily shut down one-fifth of the centrifuges Iran had at the time to purify uranium, achieving with computer code what could only have been previously been accomplished through physical bombing and explosives.[22] This attack foreshadowed the hundreds of cyberattacks that would happen all over the world in the next decade, a count that continues to escalate today.

The highest-profile example of interference in elections is the Russian Federation's interference in the 2016 United States presidential election. In 2017, the United States Department of Homeland Security confirmed that the Russian Federation interfered in the 2016 election via "a multi-faceted approach intended to undermine confidence in the American [government]."[23] Fears such as "sharia law in America", targeted attacks against minority voters, and character attacks against the Democratic Party's candidate, Hillary Clinton, were a few of the Russian methods that this report identified. There were also a number of instances where events and demonstrations were organized by Russians posing as Americans on social media.[24] It's difficult to measure the direct impact that this had on the American population. However, this report concludes that narratives pushed by the Russian information operation were promoted to the general public and had some notable effect on the population.

While this is one of the most well-known cases of Russian interference in elections, it's certainly not the only instance. Cyberattacks in Ukraine, Bulgaria, Estonia, Germany, France, and Austria over the past decade have been attributed to various Kremlin-backed hackers appearing to be

[19] UN General Assembly, "Universal Declaration of Human Rights,", 1947. Accessed July 04, 2019. http://www.un.org/en/universal-declaration-human-rights/.

[20] H.R. Rep. No. GAO-05-434 (2005). https://www.gao.gov/new.items/d05434.pdf.

[21] Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." The New York Times. June 01, 2012. Accessed July 04, 2019. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0&mtrref=en.wikipedia.org.

[22] Ibid.

[23] "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution." January 6, 2017. Accessed July 3, 2019. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[24] Ibid.

aimed at influencing election results, undermining trust in government institutions, the media, and elected officials.[25]

The balance between transparency and security is one of the central issues in discussing election cybersecurity. Without a doubt, many election management processes have been significantly improved through the application of technology. Large-scale data entry, management of voter registration data, production of ballots, and logistical planning are just a few examples of these advantages. But even though international cyberattacks have become more frequent, electoral processes are becoming increasingly reliant on the kinds of technology these attacks exploit; digital voter rolls and election results, biometric voter registration, and electronic voting machines are increasingly integrated into elections processes.[26] However, the public can quickly lose trust in any system that is a "black box" to non-experts. Thus, securing this technology means more than strong hardware and software, it also means securing the human, political, legal and procedural aspects of an election.[27] Ensuring this delicate balance between transparency and security must be one of the primary concerns of national institutions.

Previous Attempts at Solutions

UN efforts to address cybersecurity issues began in 1998 when the Russian Federation introduced draft resolution A/RES/53/70 to the UNGA on the "Developments in the field of information and telecommunications in the context of international security."[28] Now, there are over four major organs within the UN that are involved in creating cyberlaw. The General Assembly First Committee (GA1) serves as the central platform for discussions on the application of international cyber norms and State behavior, and the General Assembly Second Committee (GA2) focuses on critical infrastructure protection. Additionally, the Economic and Social Council (ECOSOC) and the General Assembly Third Committee (GA3) have centered their efforts on human rights issues resulting from State abuses of the cyberspace.[29] However, despite the valiant efforts from the General Assembly to address this issue, the ever-increasing

[25] Velde, Jacqueline Van De. "The Law of Cyber Interference in Elections." Yale Law School, July 25, 2016. Accessed July 2, 2019. https://law.yale.edu/system/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf

[26] Ellena, Katherine, and Goran Petrov. "Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Training (HEAT) Process for Election Management Bodies." International Foundation for Electoral Systems, October 2018. Accessed July 3, 2019. http://aceproject.org/ero-en/ifes-cybersecurity-in-elections.

[27] Velde, Jacqueline Van De. "The Law of Cyber Interference in Elections." Yale Law School, July 25, 2016. Accessed July 2, 2019. https://law.yale.edu/system/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf

[28] UN General Assembly First Committee (DISEC), Developments in the field of information and telecommunications in the context of international security (A/RES/53/70), 1999.

[29] Kavanagh, Camino. "United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century." United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, 2017. Accessed July 1, 2019. http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

rate of cyberattacks has led Member States to examine the challenges more seriously and press for active participation from the Security Council itself.[30]

Among the international community, the development of cyberspace "norms" (a non-binding standard of appropriate behavior for actors with a given identity) has emerged as one of the main policy tools of choice.[31] As noted in the 2015 GA1 Group of Governmental Experts (GGE) report, the "application of norms derived from existing international law relevant to the use of [the cyberspace], particularly the UN Charter and the Universal Declaration of Human Rights, is an essential measure to reduce risks to international peace, security, and stability."[32] While the creation of international norms is a critical aspect of addressing State abuse of the cyberspace, it's important to note that the lack of norms is not the problem. The General Assembly has already identified the principles that *ought* to be recognized by the international community, but the lack of clarity within these norms has created significant confusion in the international community.[33] Additionally, the lack of consequences in the General Assembly's non-binding statements about cybersecurity has allowed many State and non-State actors to disregard measures suggested by the UN.

Avenues and Hurdles for Future Solutions

Despite many positive developments and the gradual spread of cyber norms, the foundations for establishing a strong normative framework around the use of the cyberspace in the context of international peace and security seem to be faltering. They remain complicated due to the following five reasons:

1. Disagreements among States on how existing rules of international law apply to State use of the cyberspace;
2. The sluggishness of some States in moving beyond mere process to a more practical implementation of recommended norms of State behavior;
3. A lack of capacity and resources to implement some of the recommended norms and confidence-building measures;
4. A lack of awareness by policymakers in many States of the different normative processes underway within and beyond the UN relating directly or indirectly to international peace and security;
5. A deepening lack of trust among various stakeholders, undermining collaboration and cooperation.[34]

[30] Henderson, Christian. "The United Nations and the Regulation of Cybersecurity." Research Handbook on International Law and Cyberspace, 2015. Accessed July 1, 2019. https://www.elgaronline.com/view/9781782547389.00035.xml.

[31] Kavanagh, Camino. "United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century." United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, 2017. Accessed July 1, 2019. http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

[32] Henderson, Christian. "The United Nations and the Regulation of Cybersecurity." Research Handbook on International Law and Cyberspace, 2015. Accessed July 1, 2019. https://www.elgaronline.com/view/9781782547389.00035.xml.

[33] Ibid.

[34] Kavanagh, Camino. "United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century." United Nations, Cyberspace and International Peace and Security: Responding to

One way to approach this issue is by determining how current international law applies to the cyberspace. If one state uses an “internationally wrongful threat or use of force,” launches an armed attack against another nation, or threatens international peace and security, the Security Council is allowed to intervene and try to stop the violation as they see fit. The question that the Security Council must answer is when a cybercrime becomes so extreme that it falls under this aforementioned category. This lack of clarity as to what rules apply in cyberspace is one of the factors contributing to the current lack of international cyber policy. This approach could also include creating an avenue for Member States to exchange information on national policies, best practices, decision-making processes, and national organizations and structures with regard to cybersecurity.

Another possible solution is creating new international legislation to deal specifically with election and infrastructure cybersecurity. This could be manifested in measures such as requiring governments and governmental institutions to report any discovered cybersecurity vulnerabilities to the private institutions these weaknesses concern. For example, after a cyber-attack on Microsoft software in 2017, it was revealed that the US National Security Agency (NSA) had already discovered the weakness that the attacker exploited. If the NSA had disclosed the weakness to Microsoft, the company could have worked to solve the problem and potentially prevented the attack.[35] Rather than undermining international peace and security by exploiting weaknesses in other countries’ cybernetworks, the international community could promote cooperation and protect themselves and others by agreeing to disclose any vulnerability detected.

Conclusion

The sabotage of critical infrastructures and election security is a pressing global threat. The Security Council now has the opportunity to build on the previous work of the General Assembly, consider the relations of current international law and the cyberspace, and take concrete, binding action. New and innovative solutions to these problems must be proposed in order to protect democracy, human rights, and international peace.

Questions to Consider

1. How can we assist developing Member States in creating strong cyber defenses against infrastructure attacks?
2. If an international agreement is made, what will be the penalties for breaking it?
3. Can Member States that have a history of tension over cybersecurity come to an agreement on solving this issue?
4. How should the issue of State-backed hacking be addressed differently than hacking by non-State actors?

Complexity in the 21st Century, 2017. Accessed July 1, 2019. http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

[35] "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council on Foreign Relations. February 23, 2018. Accessed July 11, 2019. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

5. How can the Security Council improve the mandate, resources, or abilities of the International Telecommunications Union to address cybersecurity and infrastructure? How can the two organizations work together?

Annotated Bibliography

"Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution." January 6, 2017. Accessed July 3, 2019. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

> *This report contains an assessment of the motivations and scope of the Russian Federation's intentions regarding US elections, and their use of cyber tools to influence US public opinion.*

"Election Technology and Cyber Security: Standards, Good Practice and Guidelines." Ace Project: The Electoral Knowledge Network. April 2018. Accessed July 04, 2019. http://aceproject.org/election-technology-and-cyber-security-standards.

> *This resource compiles a list of international and national standards, good practice guidelines, example frameworks, observer outlines, academic literature, and jurisprudence regarding election security.*

"Global Cybersecurity Index (GCI) 2017." *International Telecommunications Union*, 2017. Accessed July 2, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

> *The Global Cybersecurity Index measures the commitment of countries to cybersecurity at a global level, raising awareness of the different elements of the problem, and stressing the importance of infrastructure security.*

Henderson, Christian. "The United Nations and the Regulation of Cybersecurity." *Research Handbook on International Law and Cyberspace*, 2015. Accessed July 1, 2019. https://www.elgaronline.com/view/9781782547389.00035.xml.

> *This chapter covers what has already been done within the United Nations to address cybersecurity, and also provides a general history of the issue itself.*

H.R. Rep. No. GAO-05-434 (2005). https://www.gao.gov/new.items/d05434.pdf.

> *This study covers different cybersecurity-related roles, responsibilities, and challenges that were identified by the United States Government Accountability Office in national law and policy.*

"Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council on Foreign Relations. February 23, 2018. Accessed July 11, 2019. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

> *This briefing from the International Institutions and Global Governance Program includes information on a 2017 cyber attack on Microsoft, and the subsequent role of the US National Security Agency in the attack.*

Kavanagh, Camino. "United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century." ***United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, 2017. Accessed July 1, 2019. http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.**

> *This report focuses on the UN's response to cybersecurity in the context of international peace and security. It also discusses how this relates to other UN processes and how the UN can play a role in raising awareness of the importance of cybersecurity.*

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." The New York Times. June 01, 2012. Accessed July 04, 2019. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0&mtrref=en.wikipedia.org.

> *This newspaper article focuses on Operation Olympic Games and the role that the US and Israeli government played in the first known instance of a cyberattack on critical infrastructure.*

Stewart, Emily. "This Is Now the New Normal: An Expert Explains Why Cybersecurity Risks Aren't Going Away." Vox. August 26, 2018. Accessed July 04, 2019. https://www.vox.com/policy-and-politics/2018/8/26/17782408/russia-iran-cybersecurity-threat-facebook-midterms.

> *This article reports on an interview with Theresa Payton, an expert in the field of cybersecurity and former US White House chief information officer. She discusses the current cybersecurity landscape and the role of public-private partnerships in cybersecurity.*

United Nations General Assembly First Committee (DISEC), Developments in the field of information and telecommunications in the context of international security (A/RES/53/70), 1999.

> *This is the first UN resolution that dealt with the cyberspace. It advised for the development of international cyber law, defined terms such as "information security", and called for further action from the UN.*

United Nations General Assembly, "Universal Declaration of Human Rights,", 1947. Accessed July 04, 2019. http://www.un.org/en/universal-declaration-human-rights/.

The Universal Declaration of Human Rights is a milestone document in the history of fundamental human rights, representing the common standard of achievement for all peoples and nations.

Velde, Jacqueline Van De. "The Law of Cyber Interference in Elections." ***Yale Law School*****, July 25, 2016. Accessed July 2, 2019. https://law.yale.edu/system/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf.**

This study explains the international legal framework that applies to interference in digital elections.

II. Combating the Financing of Terrorism through Non-Profit Organizations

"Money is the lifeblood of terrorism."
— Teodoro Locsin Jr., Secretary for Foreign Affairs of the Philippines (2019)

Introduction

On the morning of September 11, 2001, the terrorist group al-Qaeda conducted a series of four coordinated attacks against the United States. These attacks killed 2,996 people, injured over 6,000, set off the ensuing "War on Terror" that directly killed half a million civilians in the Middle East, and affected millions more.[36] Despite international efforts to curb this issue, terrorist attacks have only risen in number and prominence since 2001. This is partly due to the relative ease of financing these attacks. While the 9/11 attacks are believed to have cost as much as a half million dollars, most terrorist operations have much more modest budgets. The UN estimates the 2002 bombing of a Bali nightclub cost about $50,000, the 2004 Madrid train bombing cost less than $15,000, and the 2005 attacks on London's mass transit system cost under $2,000.[37] In more recent years, the 2015 terrorist attacks in Paris, France, were believed to have cost less than $10,000.[38]

Article 2.1 of the 1999 International Convention for the Suppression of the Financing of Terrorism defines the crime of terrorist financing as the offense committed by any person who:

> By any means, willfully provides or collects funds with the intention or the knowledge that they are to be used, in order to carry out [an act] intended to cause death or serious bodily injury in order to intimidate a population or to compel a government or an international organization to do or to abstain from doing any act.[39]

Thus, while terrorist groups will use some funding for actual attacks, the majority of funding that these networks require is needed to maintain and develop their organizations.[40] This organizational funding is still considered to be within the realm of terrorism funding. Terrorist financing risks also extend beyond the banking and financial sectors. According to the UN Financial Action Task Force (FATF), "The misuse of non-profit organizations (NPOs) for the financing of terrorism is coming to be recognized as a crucial weak point in the global struggle to

[36] Crawford, Neta C. "Human Cost of the Post-9/11 Wars: Lethality and the Need for Transparency." Watson Institute of International and Public Affairs, November 2018. https://watson.brown.edu/costsofwar/files/cow/imce/papers/2018/Human Costs, Nov 8 2018 CoW.pdf.

[37] "Tracking Down Terrorist Financing." Council on Foreign Relations. April 4, 2006. Accessed July 23, 2019. https://www.cfr.org/backgrounder/tracking-down-terrorist-financing.

[38] "Terror on a Shoestring: Paris Attacks Likely Cost $10,000 or Less." NBCNews.com. November 18, 2015. Accessed July 23, 2019. https://www.nbcnews.com/storyline/paris-terror-attacks/terror-shoestring-paris-attacks-likely-cost-10-000-or-less-n465711.

[39] "International Convention for the Suppression of the Financing." United Nations. December 9, 1999. Accessed July 23, 2019. https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf

[40] "FATF Terrorist Financing Typologies Report." Documents - Financial Action Task Force (FATF). February 29, 2008. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/fatfterroristfinancingtypologiesreport.html.

stop [terrorism] funding at its source.”[41] Funds, material, volunteer personnel, and public influence are key resources for both groups, which makes NPOs particularly vulnerable to abuse by terrorist networks.[42]

While current weaknesses in the NPO sector have made them particularly vulnerable to misuse, it's imperative that terrorism prevention efforts doesn't block humanitarian work. This concern was echoed by the International Red Cross Committee in a meeting regarding S/RES/2462 (2019), which was created in response to "Threats to international peace and security caused by terrorist acts."[43] The Committee's representative said: “We understand the legitimate concerns of States and their need to take measures necessary to ensure security. But, certain measures, most notably counter-terrorism legislation and sanctions, can criminalize and restrict humanitarian action.”[44]

The Effects of Legislation on Legitimate Non-Profit Organizations

Donations from NPOs are one of the largest sources of terrorist funding. One of the most significant reasons NPOs play such a large role in terrorist financing is due to a central belief within Islam, known as *zakat*, or the giving of a proportion of one's wealth to charity. While the majority of Islamic NPOs exist to help the poor and spread the charitable message of Islam, some have also been used to finance terrorism.[45] As Lee Wolosky, a former US National Security Council official, explains, "There are nefarious charities and there are good charities with nefarious people working for them."[46]

Terrorist networks will also set up illegitimate NPOs to funnel funding into their organizations. Two examples of this are the US-based Holy Land Foundation (HLF) and the US-based Global Relief Foundation (GRF). In 2001, the HLF was the largest Islamic charity in the US. In December of that year, the US government designated HLF a terrorist organization[47], and the NPO's leaders were convicted for contributing over $12 million to Hamas and $18,000 to other terrorist-sponsored NPOs. Later in 2002, the US government shut down the GRF for assisting the

[41] Jacobson, Michael. "Terrorist Financing and the Internet." Studies in Conflict and Terrorism 33, no. 4 (March 9, 2010). Accessed July 23, 2019. https://www.tandfonline.com/doi/full/10.1080/10576101003587184?cookieSet=1.

[42] "Risk of Terrorist Abuse in Non-profit Organisations." Documents: Financial Action Task Force (FATF). June 2014. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html.

[43] United Nations Security Council, Threats to international peace and security caused by terrorist acts: Preventing and combating the financing of terrorism (S/RES/2462), 2019.

[44] "Security Council Unanimously Adopts Resolution Calling upon Member States to Combat, Criminalize Financing of Terrorists, Their Activities | Meetings Coverage and Press Releases." United Nations. March 28, 2019. Accessed July 23, 2019. https://www.un.org/press/en/2019/sc13754.doc.htm.

[45] Ibid.

[46] "Tracking Down Terrorist Financing." Council on Foreign Relations. April 4, 2006. Accessed July 23, 2019. https://www.cfr.org/backgrounder/tracking-down-terrorist-financing.

[47] "Federal Judge Hands Downs Sentences in Holy Land Foundation Case." The United States Department of Justice. September 16, 2014. Accessed July 23, 2019. https://www.justice.gov/opa/pr/federal-judge-hands-downs-sentences-holy-land-foundation-case.

Taliban and listed it among the "Designated Charities and Potential Fundraising Front Organizations for Foreign Terrorist Organizations."[48]

However, terrorist funding from NPOs does not only come from Islamic charities. Globalization has drawn international NPOs into areas where terrorist networks operate, providing a framework for national and international operations and transactions that is essentially open to misuse.[49] Additionally, a large part of the NPO workforce is made up of volunteers, who are often not given a thorough background check and have little to no technical expertise. This makes NPO frameworks vulnerable to sabotage, both from hacking and infiltration. Additionally, the high level of public trust in the work done by the NPO sector has led both the international community and national governments to generally not scrutinize NPOs as consistently as other sectors. Terrorist networks abuse this public trust by piggybacking on the legitimate activities of NPOs, or by mimicking the actions of legitimate NPOs.[50]

Existing International Policy and Organizations

The FATF plays a central role in efforts to combat terrorist financing. In October 2001, just one month after 9/11, the FATF drafted eight Recommendations for the prevention of terrorist financing. In particular, Recommendation 8 states that Member States should review the adequacy of laws and regulations that relate to entities that can be abused.[51] When the FATF was in the process of creating these Recommendations, a study found that “the misuse of non-profit organizations for the financing of terrorism is coming to be recognized as a crucial weak point in the global struggle to stop such funding at its source.”[52] According to Recommendation 8, Member States should ensure that NPOs cannot be misused:

1. By terrorist organizations posing as legitimate entities;
2. In order to exploit legitimate entities as conduits for terrorist financing, such as escaping asset-freezing measures;
3. To conceal or obscure the diversion of funds intended for legitimate purposes to terrorist organizations.[53]

Within Recommendation 8, the FATF also laid out a four-pronged approach to identifying, preventing and combating terrorist misuse of NPOs. This approach focuses on:

[48] "U.S. Department of the Treasury." Treasury Department Statement Regarding the Designation of the Global Relief Foundation. October 18, 2002. Accessed July 24, 2019. https://www.treasury.gov/press-center/press-releases/Pages/po3553.aspx.
[49] Ibid.
[50] "Risk of Terrorist Abuse in Non-profit Organisations." Documents: Financial Action Task Force (FATF). June 2014. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html.
[51] "FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism." United Nations. Updated June 2019. Accessed July 24, 2019. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
[52] "FATF Terrorist Financing Typologies Report." Documents - Financial Action Task Force (FATF). February 29, 2008. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/fatfterroristfinancingtypologiesreport.html.
[53] Ibid.

1. Outreach to NPOs;
2. Supervision and monitoring of NPOs;
3. Information gathering and investigation of terrorists networks that abuse NPOs;
4. International engagement to protect NPOs globally.[54]

Following the issuing of these Recommendations, the FATF's evaluations found that only 57 percent of evaluated Member States were not compliant or only partially compliant with Recommendation 8, and a meager five percent of Member States were fully compliant or largely compliant with the Recommendation.[55]

The Terrorism Prevention Branch (TPB) of the United Nations Office on Drugs and Crime also plays a large role by monitoring the legal aspects of terrorism financing. Their duties include reviewing domestic legislation; developing Member States' abilities to prosecute and investigate terrorism financing; conducting specialized training related to freezing, seizing, and confiscating terrorist funds; and strengthening regional and international cooperation against terrorism financing.[56]

Lastly, in March 2019, the Security Council made major headway on the issue of terrorist financing by unanimously adopting S/RES/2462, "Threats to international peace and security caused by terrorist acts: Preventing and combating the financing of terrorism," the first Council resolution dedicated to this issue. This resolution takes stock of the existing international standards and requirements developed in the context of previous resolutions, such as the International Convention for the Suppression of the Financing of Terrorism (1999), the Recommendations of the FATF, and S/RES/1373 (2001), which recalls the obligation of Member States to criminalize, prosecute, and penalize terrorist financing.[57] Resolution 2462 was particularly groundbreaking because it urged all Member States to create a full assessment of the sectors most vulnerable to terrorism financing, including NPOs, and to improve the traceability and transparency of financial transactions.

Avenues for Future Solutions

In 2014, the FATF conducted a study to address terrorist financing vulnerabilities and threats faced by NPOs. They found that the NPOs most vulnerable to misuse were those operating or affecting civilians in close proximity to active terrorist threats, such as the Middle East, Asia, and Africa.[58] Additionally, they found that the countering of NPO misuse was not limited to criminal prosecution. Administrative enforcement, financial penalties, and targeted financial sanctions play important roles in countering NPO misuse.[59]

[54] Ibid.

[55] "Risk of Terrorist Abuse in Non-profit Organisations." Documents: Financial Action Task Force (FATF). June 2014. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html.

[56] "Terrorism Financing - United Nations Security Council Counter-Terrorism Committee." United Nations. Accessed July 24, 2019. https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/.

[57] United Nations Security Council, Threats to international peace and security caused by terrorist acts: Preventing and combating the financing of terrorism (S/RES/2462), 2019.

[58] Ibid.

[59] Ibid.

One potential solution to this problem is approaching it from a self-regulation standpoint and creating resources for NPOs to ensure that they are not taken advantage of. According to the book *Money Laundering Prevention*, written by financial laundering and ethics expert Jonathan E. Turner, Member States could take advantage of this public-private partnership and include NPOs in countering terrorism financing.[60] Private companies could also work with governments to monitor terrorism financing trends, sources, and methods. These resources could manifest in the form of guidelines, bi-annual reviews, the availability of technical expertise, and higher security requirements for NPO volunteers that operate in high-conflict areas.[61]

Resolution 2462 urged all States to assess their respective terrorist-financing risks, particularly by enhancing the traceability and transparency of financial transactions.[62] Member States could take advantage of public-private partnerships to increase the traceability and transparency of NPO's transactions. Further, sharing these findings with regional organizations and Member States would promote global cooperation against terrorism financing.

The main issue at hand is that international laws, regulations, and guidelines concerning the misuse of NPOs are not effectively integrated into national criminal procedures.[63] According to the FATF, while there are several tools that already exist to counter terrorist financing; the main challenge consists of implementing these tools effectively, especially in developing countries.[64] Vladimir Voronkov, Under-Secretary-General of the UN Office of Counter Terrorism, called upon Member States to make national experts and funding available to UN task forces in order to counter terrorism financing. This would give beneficiary Member States opportunities to learn good practices and provide resources to prevent and detect terrorism financing. For example, the freezing of terrorist assets is a highly effective way for Member States to stem the flow of funds. However, this is still not commonly used in many Member States. In an assessment conducted by the Counter-Terrorism Committee, they found that Member States required expert technical assistance in implementing asset-freezing policy.[65] Thus, while streamlining international policy for counter-terrorism financing might be the most time-sensible solution for the Security Council, the most effective legislation is specific to Member States' demographic, financial situation, and legal system.

Conclusion

[60] Turner, Jonathan E. "Terror Financing," in Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud. Hoboken: Wiley, 2011.

[61] "FATF Terrorist Financing Typologies Report." Documents - Financial Action Task Force (FATF). February 29, 2008. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/fatfterroristfinancingtypologiesreport.html.

[62] United Nations Security Council, Threats to international peace and security caused by terrorist acts: Preventing and combating the financing of terrorism (S/RES/2462), 2019.

[63] "Security Council Unanimously Adopts Resolution Calling upon Member States to Combat, Criminalize Financing of Terrorists, Their Activities | Meetings Coverage and Press Releases." United Nations. March 28, 2019. Accessed July 23, 2019. https://www.un.org/press/en/2019/sc13754.doc.htm.

[64] "Terrorist Financing." Documents: Financial Action Task Force (FATF). Accessed July 23, 2019. https://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html.

[65] "Terrorism Financing - United Nations Security Council Counter-Terrorism Committee." United Nations. Accessed July 24, 2019. https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/.

Terrorism, both domestic and international, is a grave threat to international peace and security. However, it cannot be handled in the same way that conventional threats have been handled in the past. Applying a humanitarian lens to anti-terror strategies will ultimately be the difference between a short-term solution and a long-term solution.

Questions to Consider

1. How can the Security Council ensure that developing countries have the effective means and resources to combat terrorism financing?
2. How can the Security Council protect religious freedom and *zakat* while still countering anti-terrorist financing?
3. What can the Security Council do to assist Member States in effectively implementing international legislation, such as FATF Recommendation 8?
4. How can the Security Council ensure that NPOs and charities won't be negatively affected by anti-terrorism financing legislation?
5. What resources can the Security Council provide to NPOs so that they are better able to monitor their own organizations and self-regulate?

Annotated Bibliography

Crawford, Neta C. "Human Cost of the Post-9/11 Wars: Lethality and the Need for Transparency." Watson Institute of International and Public Affairs, November 2018. https://watson.brown.edu/costsofwar/files/cow/imce/papers/2018/Human Costs, Nov 8 2018 CoW.pdf.

This study from Brown University tallies the total direct deaths in Iraq, Pakistan, and Afghanistan during the post-9/11 "War on Terror."

"FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism." United Nations. Updated June 2019. Accessed July 24, 2019. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20 2012.pdf.

The FATF Recommendations set standards and promote effective implementation of measures to combat terrorist financing.

"FATF Terrorist Financing Typologies Report." Documents - Financial Action Task Force (FATF). February 29, 2008. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/fatfterroristfinancingtypologiesreport.html.

This FATF study examines the means used by terrorists to raise funds and the wide variety of methods used to move money within and between organisations. The study highlights the importance of links between financial tools and wider counter-terrorist action to combat terrorist financing.

"Federal Judge Hands Downs Sentences in Holy Land Foundation Case." The United States Department of Justice. September 16, 2014. Accessed July 23, 2019. https://www.justice.gov/opa/pr/federal-judge-hands-downs-sentences-holy-land-foundation-case.

This press release details the sentences of the 2008 Holy Land Foundation case, in which their leaders are convicted of funneling funding into Hamas, a terrorist organization.

"International Convention for the Suppression of the Financing." United Nations. December 9, 1999. Accessed July 23, 2019. https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf.

The Terrorist Financing Convention is a UN treaty designed to promote the national criminalization of terrorism financing. The convention also seeks to promote police and judicial co-operation to prevent, investigate and punish terrorism financing.

Jacobson, Michael. "Terrorist Financing and the Internet." Studies in Conflict and Terrorism 33, no. 4 (March 9, 2010). Accessed July 23, 2019. https://www.tandfonline.com/doi/full/10.1080/10576101003587184?cookieSet=1.

This study shows how terrorist organizations use the Internet to spread propaganda, rally new recruits, and financing-related purposes.

Kaplan, Eben. "Tracking Down Terrorist Financing." Council on Foreign Relations. April 4, 2004. Accessed July 24, 2019. https://www.cfr.org/backgrounder/tracking-down-terrorist-financing.

This essay shows that a crucial aspect of global anti-terror efforts involves unraveling the networks that have funded attacks internationally.

"Risk of Terrorist Abuse in Non-profit Organisations." Documents: Financial Action Task Force (FATF). June 2014. Accessed July 23, 2019. http://www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html.

This typologies report examines how NPOs are at risk of terrorist abuse. The report uses case studies to increase awareness of the methods and risk of abuse for terrorism of the NPO sector.

"Security Council Unanimously Adopts Resolution Calling upon Member States to Combat, Criminalize Financing of Terrorists, Their Activities | Meetings Coverage and Press Releases." United Nations. March 28, 2019. Accessed July 23, 2019. https://www.un.org/press/en/2019/sc13754.doc.htm.

This press release covers a meeting on resolution 2462. It is a great resource to find all Member State's opinions on this resolution, the financing of terrorism, and terrorism in general. It can also provide some angles to take when writing about solutions to this problem.

'"Terror on a Shoestring: Paris Attacks Likely Cost $10,000 or Less." NBCNews.com. November 18, 2015. Accessed July 23, 2019. https://www.nbcnews.com/storyline/paris-terror-attacks/terror-shoestring-paris-attacks-likely-cost-10-000-or-less-n465711.

This article details how terrorists in the 2015 terrorist attacks in Paris, France obtained their funding.

"Terrorist Financing." Documents: Financial Action Task Force (FATF). Accessed July 23, 2019. https://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html.

This resource consolidates all FATF efforts to combat terrorist financing. This is a great resource for finding existing international legislation.

"Terrorism Financing - United Nations Security Council Counter-Terrorism Committee." United Nations. Accessed July 24, 2019. https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/.

This article talks about the mandate of the Security Council's Counter-Terrorism Committee. It also includes their factsheet on countering terrorist financing.

Turner, Jonathan E. "Terror Financing," in Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud. Hoboken: Wiley, 2011.

This book was written to address the private sector and the prevention of money laundering. Further, it shows private organizations how to deter, detect, and resolve financial fraud cases internally.

United Nations Security Council, Threats to international peace and security caused by terrorist acts: Preventing and combating the financing of terrorism (S/RES/2462), 2019.

Resolution 2462 was a groundbreaking resolution on the topic of terrorism financing. It's the groundwork for the things the Security Council will do on the topic of the misuse of NPOs. Read this resource carefully.

"U.S. Department of the Treasury." Treasury Department Statement Regarding the Designation of the Global Relief Foundation. October 18, 2002. Accessed July 24, 2019. https://www.treasury.gov/press-center/press-releases/Pages/po3553.aspx.

This statement details the ruling on the US-based Global Relief Foundation, which was designated as a terrorist affiliate in 2002.