ZYGMUN

ECOSOC

COMBATING ORGANISED CYBERCRIME

PRANIT DUA
THALEIA ANTONIOU
ANNA ZACHARIADOU

Table of Contents

I. Introduction

Cybercrime, which constitutes a part of terrorism, inherently violates the Charter of the United Nations – the rule of law, the respect for human rights, the protection of civilians, tolerance, and the ideal of peaceful resolution of conflicts. It feeds off despair, oppression, extremism, and human rights abuse, flourishing in contexts of conflict, foreign occupation, and weak State jurisdiction. It has often been cited as one of the greatest threats to international peace and security.

For these reasons, the countering of international terrorism has taken priority on the agenda of the United Nations since the 1960s and in this time, the UN has produced eighteen universal instruments to counter the issue at hand. The notion of counter-terrorism incorporates the practice, tactics, and strategies that governments, militaries, law enforcements, businesses and intelligence agencies utilize to combat or prevent terrorism. In the ZYGMUN ECOSOC, we will be approaching the counter-cybercrime strategy of combatting and preventing the organized cybercrime.

Intuitively, one may assume that such an issue is simple to grasp and overcome due to the fact that funds collected for terrorist organizations and thus cybercrime come from inherently illegal sources. However, in reality, there is a far wider spectrum with regards to acquiring financial capital. At present, there are over a hundred countries cooperating on the global war on terrorism, including attempts to close down sources of terrorist funding. As a result of this, there has been a concurrent evolution of strategies for revenue and the provision of financial support for terrorist organizations.

Contrary to popular belief, funding for terrorist organizations can be obtained from "legal sources." This includes fundraising and the legitimate collection of donations. This can be seen in Jordan's Arab Bank knowingly provided financial services that supported Hamas militants, as well as private donations to the Islamic State of Iraq and the Levant. Having said that, the majority of financial resources possessed by terrorist organizations comes from a range of criminal sources such as drug trafficking, smuggling of weapons and other goods, kidnapping, extortion, counterfeiting and fraud to computer-related offences, content-related offences and offences related to infringements of copyright and related rights.

Given this complexity, strong coordination and cooperation between states at the regional and international level is critical to effectively combat cybercrime. This can include assistance in investigation, regional bodies that cooperate towards effective implementation, and shared mechanisms to safeguard financial systems and address terrorism-financing techniques.

Cybercrime is an evolving form of transnational crime that is of growing importance to the United Nations (UN), and specifically the Commission on Crime Prevention and Criminal Justice (CCPCJ) and the United Nations Office on Drugs and Crime (UNODC). Cybercrime generates an estimated $1.5 trillion in revenue per year, and as with many crimes, it often targets the most vulnerable, with identity theft, credit card fraud, and phishing of online data being three of the most common online crimes committed. Cybercriminal activity takes place within the confines of cyberspace and is amplified by the involvement of individuals and groups specializing in

coordinated crime such as fraud and money-laundering. Because of the remote nature of cybercrime, perpetrators and victims of cybercrime can be, and typically are, located in different regions at the moment of attack. Despite the seriousness of cybercrime and its relation to other forms of organized crime, there is no internationally recognized definition of cybercrime.

While there is no internationally agreed upon definition of cybercrime, the UNODC working description of cybercrime is "cyber-dependent and cyber-enabled offences, including serious human rights violations through online child exploitation and abuse."[1] With cyber-dependent crimes, information and communications technology (ICTs) infrastructure is often used to support malware, attacks on infrastructure, and data overloads or distributed denial-of-service (DDOS) attacks, designed to take a website offline. Cyber-enabled offenses can also occur offline but be facilitated by ICT, and often revolve around fraud, online drug exchange, and money-laundering. The wide range of offenses that can fall under cybercrime has also facilitated its use in transnational organized crime and other large criminal enterprises, including causing damage to a Member States' security infrastructure. As indicated by UNODC, malicious cyber-based offenses such as fraud, drug exchange, and money-laundering typically circulate around "offences against confidentiality, integrity, and availability of computer data and systems, computer-related crimes, content-related offences, and offences tied to infringement of copyright and related rights."[2]

II. Definition of Key Terms

a) Cyber: Anything involving, using or relating to computers, information technology, virtual reality or the internet.[3]

b) Cybercrime: Any criminal activity that involves computers, the internet, or a network. The computer may have been used in the commission of the crime or it may even be the target. Cybercrimes or computer-oriented crimes may threaten a person, a company, a nation's security or it's financial state. [4]

c) ICT: Information and Communication Technology is a broader term for Information Technology (IT), which refers to all communication technologies such as the internet, computers, wireless networks, cell phones,n video-conferencing, software, social networking, and other applications or services that allow users to access and manipulate digital information.[5]

---

[1] UNODC, Global Programme on Cybercrime, 2018.
[2] Ibid.
[3] Dictionary.com. "Definition of Cyber | Dictionary.Com." Www.Dictionary.Com, www.dictionary.com/browse/cyber.
[4] Dennis, Michael Aaron. "Cybercrime." Encyclopedia Britannica, 19 Sep. 2019, https://www.britannica.com/topic/cybercrime.
[5] "Information and Communication Technologies (ICT)" Agricultural Information Management Standards (AIMS), http://aims.fao.org/information-and-communication-technologies-ict.

III. General Overview

a) Money Laundering

Terrorist organisations exploit the current financial system in order to disguise the illegal origins of their wealth and protect their assets in order to avoid the suspicion of law enforcement agencies. This is referred to as money laundering, which the International Monetary Fund (IMF) defines as "any transaction or series of transactions that is designed to disguise the nature/source of proceeds derived from illegal activities, which may comprise drug trafficking, terrorism, organised crimes, murders, fraud, etc."

Although terrorists are not overly concerned with concealing the origins of their money, much of their focus is concentrated on disguising its destination and purpose for which it has been collected. Therefore, the ability to prevent and detect money-laundering is a highly effective means of identifying and disrupting terrorist activity. It is an integral sub-topic to the question at hand and must be taken into consideration when devising policies towards combatting the financing of terrorism. Delegates should consider what intelligence, technology, and investigate strategies can be utilised to detect such activity.

Countries tend to have varying indicators of what is considered to be suspicious activity regarding the collection and movement of funds. They tend to include:

1. Monetary transactions that are inconsistent with account's past deposits;
2. Transactions of high volume that lack a logical justification;
3. Transactions that come from, go through, or transit through locations of concern– this may include sanctioned, blacklisted, or typically non-cooperative states
4. Corporate layering – transfers through and between multiple accounts of related entities for no apparent reason;
5. Inapparent fundraising activity;
6. Usage of multiple accounts to transfer funds to the same, individual source;
7. Unexplainable clearing of third-party cheques;
8. Transactions between accounts that have no logical economic purpose as there is no link between the parties involved;
9. Overlapping similarities associated with different addresses, references, and financial activities;
10. Reverse transactions.

Having said that, these indicators must be analysed in context with other factors as it may be difficult to determine if these suspicions are linked with terrorist activity or organised crime. It is important to recognise that while, in the majority of cases, applying frameworks broadly intended to combat money laundering can be efficacious, the primary focus of the resolution should be aimed at decreasing the inflow of financial capital to terrorist organisations; this is, again, because terrorist organisations care little about the source of funding, but rather what they can be used for.

b) Cryptocurrency

Since 9/11, the majority of states have strengthened their enforcement of anti-money laundering regulations. This has resulted in a significant reduction in the ability of terrorist organisations to effectively rely on formal banking and money transfer services. However, this may consequently lend to terrorist organisations utilising digital cryptocurrencies as they tend to heavily support anonymity. An example of this may be Bitcoin, a service where users are identified by a string of random numbers rather than their personal information. These services also extend beyond Bitcoin to other platforms that better align with terrorists' needs, such as Omni Layer, BlackCoin, and Monero, which are touted as even more private and secure. With an increase in legal and financial risks that accompanies formally funding terrorist organisations, the robust and anonymous style of cryptocurrency may enable donations to be a significant source of capital again.

It is important for delegates to address cryptocurrencies as its use may undermine the previous success of strategies to combat the financing of terrorism. This may be done through increased international law enforcement in cybersecurity domains, as well as enforcing transparency to site regulators while continuing to preserve public privacy and anonymity.

c) Funding of online terrorist activity

When constructing policies in the hopes of tackling the financing of cybercrime, it is crucial to take into consideration the variety of techniques utilised so as to ensure a holistic approach. Here is an elaboration of certain methods:

I. Misused Humanitarianism and NGOs

Humanitarian charities are an easy strategy to disguise financial activity. A concrete example of this is illustrated with Hamas, a political organisation and militant group founded in 1987 that seeks to replace Israel with a Palestinian state. It seeks the establishment of an Islamic Palestinian State, covering Israel, the West Bank and Gaza Strip, and currently governs Gaza independent of the Palestinian Authority.

Hamas is currently the second wealthiest terrorist organisation with an annual income of approximately 1 billion USD, the majority of which is generated through donations. This is owed to the fact that the organisation is notorious for taking advantage of NGOs, charities, and social programs. They have promoted advertisements towards supporting orphans and building schools while, in reality, these are merely channels for Hamas to finance their activity. This issue is especially prominent in the Middle East because charitable contributions fulfil one of the pillars of Islam (zenet) and thus, donations are widely regarded as a responsibility in this region. However, this

generosity has often gone amiss and unfortunately, can be difficult to tackle as religious organizations view this as a sensitive issue.

IV. Major Parties Involved and their Views

a) Russian Federation

In 2015, a group of Russian hackers successfully stole £650 million from several worldwide-based banks. This procedure took two years to be well prepared and established. According to the hackers, the software they used was a malware that gave them access to all the information of secured bank offices, as well as access to the staff's computer systems, which aided them in withdrawing money successfully.

Kaspersky Lab, a Russian cybersecurity firm, was able to uncover the scam. A spokesperson of the firm commented: "The plot marks the beginning of a new stage in the evolution of cybercriminal activity, where malicious users steal money directly from banks, and avoid targeting end users."

b) Japan

Japan's government released their new cybersecurity strategy and has been updating it every few years since its initial release back in 2013. The new strategy mainly targets the cybersecurity of critical infrastructure and urges Japanese businesses to carefully practice cybersecurity in aims of helping Japan's innovation and economic growth. The new strategy also encourages the industry to invest more money in cybersecurity for business operations, innovation and risk management, and therefore seeks the establishment of a company- wide budget concerning cybersecurity. The Japanese capital Tokyo is encouraging cybersecurity by claiming to reduce a company's corporate tax if they can prove to include cybersecurity measures in their IT investments.

The new cybersecurity strategy in Japan will also include practices that are the most convenient for companies to use in communicating with their C-suite and incorporate cybersecurity within their operations, and the strategy will make sure to provide companies with tools allowing them to identify cybersecurity risks and threats.

c) WannaCry Ransomware

On May 12 2017, a cyber-attack called WannaCry Ransomware happened, which targeted machines running Microsoft Windows operating systems. More than 150 countries' companies and individuals were affected in addition to multiple large organizations and government agencies on a global scale, such as the National Health Service in England as well as Renault-Nissan. Affected systems faced encrypted data and a message from the hacker demanding payments using the cryptocurrency Bitcoin, or else

the attacker threatened to increase the cost and deprive the affected companies from accessing their own files and information.

The WannaCry Ransomware affected mostly Russia, Ukraine, Taiwan, India, and the National Health Service in England. The cyber-attack was stopped by Marcus Hutchins, a 23-year-old cybersecurity researcher, who discovered the malware's kill switch accidently in the script and thus saved the internet.

V. Relevant Resolutions, Treaties and Organizations

a) Financial Action Task Force (FATF)

The Financial Action Task Force (FATF)[6] was formed at the 1987 G7 Summit in Paris as an intergovernmental organization with a specific aim to develop policies towards combatting money laundering, an initiative whose mandate extended to include terrorism financing following the 9/11 attacks in 2001. The FATF has set standards that ensure states have effective legal, regulatory, and operational measures that protect the integrity of the international financial system. They also monitor implementation of said measures in member states.

Moreover, the FATF has formulated lists of countries that are noted to not have taken adequate action towards combatting the financing of terrorism. These are formally known as the FATF Blacklist, regarded as "call-for-action nations," that only includes North Korea and Iran; and the FATF Greylist, regarded as "other monitored jurisdictions" which lists the Bahamas, Botswana, Cambodia, Ghana, Iceland, Mongolia, Pakistan, Panama, Syria, Trinidad and Tobago, Yemen, and Zimbabwe.

The FATF has also formed the Forty Recommendations on Money Laundering and the Nine Special Recommendations on Terrorism Financing, setting an international standard of measures, actions, and principles regarding combatting the financing of terrorism. These recommendations are intended to be implemented in states through national legislation.

Given the scale of the issue, the Security Council has a long record of action. They have been able to establish principles of cooperation and targeting, as well as to offer criticism, assistance, and pressure on affected states. Having said that, there has been wide room for interpretation and the application of these principles vary between each state. Delegates should consider previous attempts toward action and explore how the international community can take on more responsibility towards an effective response.

b) International Convention for the Suppression of the Financing of Terrorism[7]

[6] https://www.fatf-gafi.org/countries/
[7] https://www.un.org/law/cod/finterr.htm

This is the keystone document for international action regarding the financing of terrorism, drafted in 1999 and coming into action in 2002. The convention criminalizes the act of financing acts of terrorism, as well as provides a definition for this crime. It also promotes police and judicial cooperation, such that member states are not allowed to utilize bank secrecy as a justification to conceal transactions. The treaty has been ratified by 188 states and thus, is viewed as one of the most successful international agreements. Having said that, it mostly establishes principles and proposes a framework rather than the actual implementation of action.

c) Security Council resolution 2178 (2014)[8]

This was an initiative promoted by the Obama Administration and had won unanimous support from the Security Council. This resolution interprets the issue of terrorism with a more sophisticated eye, imploring that member states specifically disrupt terrorist-financing activities linked to financial transaction and to criminalize, under domestic law, the financing of terrorist travel. This comes from the fact that many terrorist organizations have "safe havens" that are able to send money abroad. For example, ISIS was able to coordinate transfers between sympathizers in Saudi Arabia, to active terrorists in East Asia, Europe, and the United States.

d) UN Office of Counter-Terrorism (UNOCT)

In 2017, the Security Council formed the UNOCT as a focal group for the implementation of global-counter terrorism strategies, as well as the identification of terrorist organizations' financing strategies. The UNOCT is able to coordinate and offer recommendations towards combating the issue but it does not hold the jurisdiction to demand action.

e) The Terrorism Prevention Branch (TPB)

The UN also has also formed the TPB, a branch of the United Nations Office on Drugs and Crime (UNODC). It provides legislative and technical assistance to member states regarding counter-terrorism, as well as conducts studies on the scale and nature of illicit terrorist finance and planning. On the request of the Security Council, the TPB can also investigate specific problems and quests; however, it has no authority to demand that member states cooperate with its investigations.

[8] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2178.pdf

VI. Questions to Consider

1) With the rapid development of technology and the internet, can laws preventing cybercrime keep up with such expansion?
2) To what extent do governments get involved with cybercrimes?
3) Should people get educated about cybercrimes? How?
4) Can cyber crimes ever be eradicated?
5) Do you think, for security reasons, everything that happens on the Internet should be analyzed by the public security services? If so, then how is internet users' personal privacy safeguarded?
6) How secure is digitally stored sensitive data, and how can potential hacks be investigated?
7) How does your country deal with cybercrime?
8) What internal policies and legislations has your nation implemented to fight cybercrime?
9) Has your country been a victim of cybercrimes, has it initiated one?

VII. Conclusion

The international community has taken important steps to respond to cybercrimes in all its forms, but significant challenges remain. Criminal justice responses to cybercrime will require a global approach. Everyday people across the world fall victim to cybercrime, and victims of such activities include individuals, large businesses, and even governments. The nature of the crimes have evolved, and now provide a tremendous amount of illicit revenue to individuals and cybercrime networks. International and regional frameworks are in place to address the issue, but meetings of the CCPCJ and open-ended intergovernmental expert groups have called for an increase in research, coordination, and capacity-building techniques due to the rapid expanse and development in communications technology. Coordination, information-sharing, and collaboration between Member States may be able to curb the effects of cybercrime and develop resilient legislation. Criminal justice responses to cybercrime vary depending on the Member State, but it would be in the best interest of developed states to assist developing states with their cybersecurity infrastructure, as the integrity of one state's security affects the security of all.

VIII. Bibliography

"African Union Convention on Cyber Security and Personal Data Protection." https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

Al-Turiri, Abdulrahman. “Qatar's Dubious Ties to Terrorist Groups Justify Its Boycott.” The Arab Weekly, 23 May 2020, https://thearabweekly.com/qatars-dubious-ties-terrorist-groups-justify-its-boycott.
Charter of the United Nations (1945). http://www.un.org/en/documents/charter/index.shtml.
Council of Europe (2001). Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list.
Cybercrimedata AS. (n.d.). Cybercrime Law. http://www.cybercrimelaw.net/un.html.
“Cyber Norm Emergence at the United Nations” UN Economic and Social Council Press. http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.
“Cyber Warfare”. UN News Center. http://www.un.org/press/en/2014/gadis3512.doc.htm.
Dion-Schwarz, Cynthia, et al. “Terrorist Use of Cryptocurrencies.” RAND Corporation, 27 Mar. 2019, www.rand.org/pubs/research_reports/RR3026.html.
European Commission. “Cybercrime.” https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.
Fassihi, Farnaz. “U.N. Security Council Asks Nations to Adopt Laws on Terror Financing.” The Wall Street Journal, Dow Jones & Company, 29 Mar. 2019, www.wsj.com/articles/u-n-security-council-asks-nations-to-adopt-laws-on-terror-financing-11553818459.
“History of the FATF.” Financial Action Task Force (FATF), 2019, www.fatf-gafi.org/about/historyofthefatf/.
“International Association of Cybercrime Prevention.” http://www.cybercrime-en.org/about-us-cyber-crimes.
Kaplan, Eben. “Tracking Down Terrorist Financing.” Council on Foreign Relations, 4 Apr. 2006, www.cfr.org/backgrounder/tracking-down-terrorist-financing.
Katharina.kiener-Manu. “Organized Crime Module 1 Key Issues: Activities, Organization, Composition.” Organized Crime Module 1 Key Issues: Activities, Organization, Composition, www.unodc.org/e4j/en/organized-crime/module-1/key-issues/activities-organization-composition.html.
Plaut, Martin. “After Decades of UN and Self-Imposed Isolation, Eritrea Is Coming in from the Cold.” Quartz Africa, 14 Nov. 2018, https://qz.com/africa/1463506/un-security-council-lifts-eritrea-sanctions-arms-embargo/.
Popper, Nathaniel. “Terrorists Turn to Bitcoin for Funding, and They're Learning Fast.” The New York Times, 18 Aug. 2019, www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html.
Safa., Zaben. “United Nations Office on Drugs and Crime.” Crime Prevention, www.unodc.org/unodc/en/justice-and-prison-reform/CrimePrevention.html.
“Security Council Unanimously Adopts Resolution Condemning Violent Extremism, Underscoring Need to Prevent Travel, Support for Foreign Terrorist Fighters | Meetings

Coverage and Press Releases." United Nations, 28 Sept. 2011, https://www.un.org/press/en/2014/sc11580.doc.htm.
"Statement by China on Cybersecurity at the the 68th UNGA" UN Office of Disarmament Affairs, http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf.
Stempel, Jonathan. "Arab Bank Terrorism Case Ends as U.S. Court Voids Jury Verdict." Reuters, 9 Feb. 2018, www.reuters.com/article/us-arab-bank-decision-idUSKBN1FT26Z.
"Xi Jinping, Obama Talk Cybersecurity". Al Jazeera. http://america.aljazeera.com/watch/shows/live-news/2015/9/xi-jinping-obama-talk-cybersecurity.html.
Zehorai, Itai. "The Richest Terror Organizations in the World." Forbes, 29 Jan. 2018, www.forbes.com/sites/forbesinternational/2018/01/24/the-richest-terror-organizations-in-the-world/#3d18ef257fd1.