HISAR SCHOOL

JUNIOR MODEL UNITED NATIONS 2022

“Endorsing Accountability: Reapproaching Neglected Urgencies”

Drugs and Crime

Restricting cybercrime and money laundering aimed at fostering terrorism

ELIF EREN

Forum: Drugs and Crime (SA-1)

Issue: Restricting cybercrime and money laundering aimed at fostering terrorism

Student Officer: Elif Eren

Introduction

With the rapidly growing digital world and internet, criminals have found ways to continue their operations through different alternatives. The internet has become a major tool for criminal organizations to fund, plan, and coordinate acts of terrorism, spread false information, and create connections between terrorists since it provides them with a borderless space. The Internet provides a great space for terrorists to anonymously operate and pose threat to digital systems of governments and privacy of the people. As the rapid development of such technologies catalyze cyber crime and money laundering, it is now essential to tackle the issue.

Various United Nations bodies and organizations have been asserting support to help the vulnerable who are getting negatively affected by the issue, curb the severity of the issue, and identify and disrupt the operations of such terrorist groups however, efforts have failed to stop this issue due to the complex nature of it.

Definition of Key Terms

Cybercrime: According to the United Nations Office of Drugs and Crime, cybercrime is an "evolving form of transnational crime." They are criminal operations taking place in a borderless realm of cyberspace. According to the European Commission, cybercrime has three broad definitions. The first one is "crimes specific to the internet", which are attacks against information systems or fake bank websites to gain access to victims' accounts. The second one is "online fraud and forgery" which includes spams and malicious codes. The third one is "illegal content", which includes activities such as child abuse material and the facilitation of drugs online.

Money Laundering: Illegally transferring a large amount of money earned through methods such as drug trafficking or terrorist funding which seem to have been deposited legitimately. The development of new technologies such as blockchain provides anonymity for such transfers and removes third parties such as governments, making it easier for terrorists to operate and hide their identities.

Forgery: The illegal copying of a banknote or an official document.

Law Enforcement: Making sure that law is obeyed and necessary actions are taken in case of disobedience.

Smurfing: Used in money laundering, smurfing is when a large quantity of money is divided and transferred separately from and to multiple accounts to reduce suspicion that may arise due to a large amount of money transfer.

Cryptocurrency: Cryptocurrency is a digital currency and is a decentralized system, meaning that there are no third parties such as banks or governmental institutions involved.

Financial system: A financial system includes institutions such as banks, government treasuries, stock exchanges, and insurance companies. Money launderers have to transfer the illegitimate money through such institutions.

Anti-money laundering index (AML Index): Each year, the Basel Institute of Governance (an independent non-profit to prevent corruption and financial crime) prepares an anti money laundering index (AML Index) from data collected from organizations such as the World Economic Forum and World Bank. This index is out of 10, with a higher grade meaning that the country is more vulnerable to money laundering. As countries such as Myanmar, Haiti, DR Congo and Afghanistan have the highest (most dangerous) scores, countries such as Norway, Denmark and Andorra have the lowest (safest) scores.

Cookies: Cookie policies are present in most websites. They are text files with small pieces of data regarding the visitor. So if cookies are accepted, people agree to share basic information regarding themselves - such as their browsing history, location and device details - with the website owner, which can be easily abused by criminals in cyberspace.

General Overview

Money Laundering

Money laundering is a way in which terrorist groups transfer illegal money through financial institutions. While executing this complex process, money is transferred to and from a legitimate source in order to prevent any suspicions. This act provides a financial network among terrorist groups and funds such groups' illegal activites and enhances their abilities which generate more crimes and consequently affect the peace and security of countries and the stability of their economy.

Stages of Money Laundering

Money laundering involves three stages: placement, layering, and integration. During the placement step, the money, acquired from illegal acts such as bribery, theft, or corruption, is placed into the financial system. During this step, the launderers use legitimate businesses such as car washes to conceal their identities. Also, launderers use a technique called "smurfing" to break down the large amount of money and transfer it to multiple bank accounts from multiple sources to reduce suspicion. The second step is the layering. This is when criminals make it difficult for institutions to identify the source so that the money can be transferred. This is done with the use of other investment tools such as stocks and real estate to make the money untraceable.

The third step is the integration. During this step the money is successfully cleansed. This money is ‘integrated’ into the financial system as high-priced commodities such as cars or artworks.

Where Can Money Laundering Occur?

This process can be done all over the world. However, terrorist groups prefer to do this in states with weak anti-money laundering programmes, a lack of monitoring and weak oversight such as Afghanistan. Although not prevalent, cryptocurrency has also helped such terrorist groups as the blockchain technology removes the third party, or in other words government banks, and helps terroist groups transfer money with ease. Chainanalysis found out that approximately 2.8 billion United States Dollars (USD) in Bitcoin were moved by criminals, only in 2019.

Cybercrime

Large and borderless computer networks create a global cyberspace for terrorists. In this cyberspace, terrorists can maintain their anonymity, engage in hidden communication and illegally transfer and store data.

Financing

One of the ways that terrorists finance their actions is through fake establishments. Some terrorist groups establish fake charities and advertise their charities through social media and mass mailings (which are gathered with the acceptance of Cookies in insecure websites, in which the site owner can gain access to some of the information of the user) to recieve donations and use that money to fund their activities. Also, there are several payment tools that are easily hackable. Terrorists use e-commerce websites, in which many people include their personal and credit card details, and make the use of data leaks (which occur in insecure websites) to finance their activities. Also with the use of platforms such as DarkWeb, terrorist groups can easily hide their identities and buy and sell illicit weapons, drugs and many mroe for profit in order to expand their budget to operate.

Attacking

Through malicious software and computer viruses, terrorists can cause a lot of damage to both personal computer networks and the networks of governments. For example, the Code Red Worm virus impacted a million servers and caused 2.6 billion USD in damage. Or in 2000, DoS attacks stopped big websites such as Amazon, eBay and Yahoo. Most people, without being aware, increase their computer system’s vulnerability by not protecting their data or falling for traps set by terrorist groups through spam mails and notifications, which make it easier for terrorists to execute their attacks.

As countries' reliance on digital systems increase, there is an increasing risk in cyber attacks. For example, many terrorist organizations attack national defense systems and air traffic control systems. Terrorists can engage in attacks against computer systems and lead to the blocking of banking systems, production processes, public administration, and military weapon systems due to the lack of necessary security and privacy measures taken by governments.

Propaganda

With the help of the internet, terrorists can also spread out racist, discriminative, and abusive content anonymously. Through pamphlets, audio recordings, magazines, videos and animations and by abusing the right to freedom of speech terrorists can easily spread out their content. In today's world, televisions and radios go through verification steps to ensure that abusive content is not being shared; however, with the presence of open social media platforms such as Facebook, Instagram and Twitter, extremist views can easily be distributed among millions of people.

Also, the spread of wrong news and rumors are prevalent in social media platforms. Such news can lead to political polarization and catalyze conflicts which can help terrorist groups enhance their control and abilities.

Recruitment and Training

Terrorist groups can recruit and train people for terrorism since the internet provides them with infinite power to voice themselves. Open platform allow terrorists groups to form networks from all around the world. Groups can recruit people from around the globe or form connections among each other and train them to expand their power. For example, this can be done with the anonymous sharing of online manuals on how to make illicit firearms or explosive devices.

Targeting

By allowing "Cookies," many agree to share details such as their location or device details. With the use of fake websites that require Cookies, website owners can easily gain access to such information. Also, many websites and applications need allowance to access important information such as the location of the user and many people accept such requests without consideration, which allows terrorist groups to target their victims. Also, by gathering email details from a targeted audience, terrorists can create mail lists to use in mass mailings to market their fake establishments and finance their actions.

Major Parties Involved and Their Views

United States of America (USA)

The USA has been one of the first countries to criminalize money laundering (in 1986). Especially after the September 2001 terrorist attacks, the US has taken strict measures to combat money laundering and has required all financial institutions to adopt anti-money laundering programmes. All institutions also require strict customer identification programmes to verify the identities' of customers. The US has a system called the Suspicious Activity Reports (SARs) which is used whenever a large, suspicious transaction is made. The Financial Crimes Enforcement Network is the financial intelligence unit of the US and mainly focuses on money laundering. For cybercrime, the US has the Federal Bureau of Investigation (FBI). One of the FBI's main purposes is to investigate cyber attacks. The FBI works with victims, collects and shares intelligence, and prevents other parties and groups from stealing financial and intellectual property.

China

Due to its large population, China also suffered from a lot of money laundering cases. Just recently, on January 26 2022, China has launched a 3 year campaign to enhance national security and tackle money laundering. This campaign is led by the national bank, People's Bank of China and the Ministry of Public Security. This campaign aims to strengthen financial intelligence in terms of how they store identity and trading data and have stricter monitoring on comprehensive information regarding customers. It also covers all types of money transfer related firms such as brokerages and insurers. Regarding cybercrime, China has voiced support to the Intergovernmental Expert Group within the UNODC (which works on analyzing cybercrime cases and maintaining international cooperation), and also encouraged other member states to share their experiences on cybercrime cases, law enforcement and criminal justice.

Afghanistan

Afghanistan is on top of the AML Index with 8.22 out of 10 in the 2020 index, meaning that the country is suffering from a lot of money laundering cases and has a vulnerable financial system. Especially with the latest security issue in the country and the emergence of the Taliban, the country has been suffering from a great lack of safety and proper governmental institutions, however the index in 2021 is uncertain as Afghanistan was not involved in the latest one. Issues such as human trafficking, lack of equality and violence have all been prevalent in Afghanistan, catalyzing such terrorist acts. Due to the Taliban takeover, financial intelligence units cannot process in Afghanistan. The Taliban itself has made millions of dollars from drug trade and money laundering processes while fighting the government. The lack of action plans is highly concerning and the lack of a functional governmental system and financial system is hindering any progress made towards tackling this issue.

Myanmar

The Global Cyber-Safety Index combines the data of the Basel AML Index, the Cyber Exposure Index, and the National Cyber Security Index (NCSI) to reach a conclusion regarding the preventative measures taken towards tackling the issue of cybercrime. In this ranking, Myanmar scored 2.2 out of 10 (the lower being the worse). The reason for this is that the government infrastructure focused on law enforcement and regulation in Myanmar is very weak. There are barely any consequences for criminal activities and little to no monitoring for the breach of safety and security regulations. An enhancement to law enforcement is an urgent need in Myanmar.

Treaties and Events

UN Security Council Resolution S/RES/2341 (2017)

This resolution is regarding the protection of critical infrastructure from terrorist attacks. Issues such as awareness, effective and fast response to attacks, the establishment of terrorist acts as criminal offences in their laws and international collaboration of member states are discussed.

UN Security Council Resolution S/2015/939

This resolution is targeted towards tackling the recruitment of terrorists. It focuses on tackling the violence caused by terrorist attacks.

Convention on Cybercrime

Also known as the Budapest Convention on Cybercrime, this convention is the first international convention to mainly focus on crimes committed in a digital medium. 65 states have ratified this convention which touches upon issues such as: computer related fraud, abusive material and network security.

Evaluation of Previous Attempts to Resolve the Issue

Anti-money laundering (AML) Compliance Programme is present in several countries. AML programs include important points such as monitoring of accounts, user policies, internal operations and reporting money laundering incidents. These programmes aim to tackle fraud-related risks that money laundering operations have, as well as terrorist financing. Banks, cryptocurrency exchanges, e-wallets, payment and credit companies mostly have them in More Economically Developed Countries (MEDCs), however such programmes do not exist in Less Economically Developed COuntries (LEDCs) due to the required resources and technology.

Also the UNODC has been organizing trainings in North America, North and Eastern Africa, Middle East and South East Asia to help identify digital evidence of terrorist acts such as drug trafficking. The Intergovernmental Expert Group within the UNODC works on maintaining international cooperation by bringing together policy makers and diplomats to discuss the effects of cybercrime and possible solutions.

There have been several resolutions passed by the Security Council regarding preventative measures to tackle activities aimed at fostering terrorism as stated in the previous section. Resolution 2341, passed in 2017, focuses on the protection of infrastructure from terrorist attacks. It also includes important points such as immediate actions towards attacks, the enhancement of law enforcement and education. One other resolution passed in 2015 focuses on the threats of terrorist attacks and also the training of terrorist groups.

Possible Solutions

Especially against cybercrime, safe digital systems should be ensured. Softwares must be built to track abusive materials, cybercrime activities and stricter montiorings should be built to ensure that money transfers are safe to avoid money laundering activities. Authorities should have sufficient power to identify foreign attackers, break encryption (since terrorists use encrypted communication systems such as Telegram), and engage in the search of computer data. Considering that countries that are suffering from aforementioned issues have a common aspect, which is a poor judicial system, law enforcement should be enhanced so that such acts don't go neglected. Also international cooperation should be maintained among Member States, United Nations and important organizations such as the International Criminal Police Organization (INTERPOL). Governments should encourage innovative cyber security solutions and collaborate with private sector companies. Awareness is also a key part. Educational seminars for preventative measures carry out huge importance. Issues such as spam mails, the vulnerability of data, the provision of personal details such as credit card information in unreliable sources and phishing can be minimized with sufficient awareness.

While coming up with solutions, delegates must make sure that clauses are applicable for LEDCs as previous attempts were mostly applicable in MEDCs as they require great financial resources.

Bibliography

"Anti-Money Laundering (AML) Compliance Program: 5 Key Components". *Sumsub*,

"Anti Money Laundering (AML) In United States Of America". *Bankersacademy.Com*,

"Basel AML Index". *Index.Baselgovernance.Org*, 2021,

*"*China Tightens Anti-Money Laundering Rules For Financial Firms", *Reuters*, 2022

"Convention On Cybercrime - Wikipedia". *En.Wikipedia.Org*,

"Cybercrime Documents". *Unodc.Org*,

"Cyber Crime | Federal Bureau Of Investigation". *Federal Bureau Of Investigation*,

"Cybercrime". *Migration And Home Affairs*,

"Cybersecurity | Office Of Counter-Terrorism". *Un.Org*,

Group, Global. "Anti Money Laundering 2021 | Laws And Regulations | USA | ICLG". *International Comparative Legal Guides International Business Reports*, 2021,

"Index". *United Nations : Office On Drugs And Crime*, Lazic, Marija. "27 Informative Money Laundering Statistics In 2022". *Legaljobs.Io*, 2021,

"Major Money Laundering Countries - Sanction Scanner". *Sanctionscanner.Com*, 2020,

"Money Laundering". *Investopedia*,

Ogun, Mehmet Nesip et al. "TERRORIST USE OF CYBER TECHNOLOGY". *Dergipark.Org.Tr*,

"The Process And Stages Of Money Laundering Explained". *St Pauls Chambers*, 2021,

Sharma, Shweta. "Which Countries Are Most (And Least) At Risk For Cybercrime?". *CSO Online*,

Sieber, Ulrich. "International Cooperation Against Terrorist Use Of The Internet". *CAIRN INFO*, 2006,

Weimann, Gabriel. "Cyberterrorism: How Real Is The Threat?". *Usip.Org*, 2022,