XXVII
TECMUN Jr.

Counter-Terrorism
Committee

Delegate,

Regardless of this being your first, second, fifth or last TECMUN, I believe in every single one of you and your ability to make this your best model and have the best time so far. These three days will be exhausting, mind-challenging, unique and a big opportunity to prove to yourself and the committee that what you can think, propose, investigate and do can and will change the world and its society someday. This task will not be easy, but it is in your power and your attitude to make sleepless nights, all those hours of investigation, position papers, etc. be worthwhile. For months you have been preparing yourself for this, make it notice.

Delegate, this is your chance to think outside of the box, to break your standards, to be yourself, to beat the system, to express your unique, creative ideas and to get out of your comfort zone. It might get scary and nerve-racking at times, but don´t let those thoughts stop you from expressing yourself, because unconfidence, hesitation and fear will always be the hardest things to overcome, but doing so, will always bring the best outcomes. I expect you to trust the model and yourself completely, to learn a variety of topics, to come out with another perspective of what is happening around the globe and with the ability to analyse and solve these problems in the best way possible.

Finally, remember the world is in the hands of the youth; and if we do not learn how to take profit of this and make it a better place, then no one will. We have a lot of power, your voice does make an impact and does change the perspective of people, so do not be afraid to speak out-loud and express your thoughts. Be open and willing to learn in this model, you will face some obstacles, opposing opinions, stressful situations, compete against the clock, but in the end, that is what will make it memorable. Cease this moment, and learn to take advantage of whichever positive aspect you might find in the way, believe in yourself and what you can bring to the model and the impact that it will leave on a lot of people, because I assure to you, I do.

Nuria Vidal Castillo

President of the Counter Terrorism Committee

XXVII TECMUN Jr.

Background of the Counter-Terrorism Committee

The Counter-Terrorism Committee (CTC), compounded by the 15 United Nations Security Council members, was established on September 28th 2001. It was founded as a result of the United Nations Security Council's Resolution 1373. The Counter-Terrorism Committee works to bolster the abilities of the United Nations' permanent members in order to prevent terrorist acts and the achievement of international security fixating on extremism. Its main goal is to implement measures to reinforce their political and institutional capabilities to counter terrorist actions in a regional, national and international manner. Such as criminalizing the financing, assistance and supporting of terrorism and enhancing the cooperation to investigate, detect, arrest, extradite and prosecute those involved in terrorist acts in any shape or form.

Topic A

Measures to ensure security on the internet in Southeast-Asia due to the ISIS recruiting of civilians to join terrorist groups through social media and the internet

By: Nuria Vidal Castillo

Introduction

The Islamic State of Iraq and Syria (ISIS) is a militant jihadist religious group of civilians that claim to have military, political and religious authority over all Muslims. ISIS was founded in 1999 by Abu Musab al-Zarqawi and since 2003, al-Zarqawi pledged allegiance to ISIS members by leading suicidal extremist acts which had the purpose to get rid of the United States' forces in Iraq, which have henceforth remained. People belonging to ISIS have ever since committed over 70 registered attacks in more than 20 countries. The consequence of this extremist group's existence is to serve Allah and free al Sunni Arabs in occasions by torturing, bombarding, kidnapping, destroying and/or affecting anyone or anything that does not agree with their intends. Terrorist groups such as Al-Qaeda have been present in Southeast Asia since 2001, existing grave encounters between Southeast Asian countries and ISIS, such as the battle held in the Philippines in 2017.

In sites of the Islamic State losing its territorial strongholds in Iraq and Syria, they have begun to reactivate various measures to regain its territorial and political power; one of them being the recruitment of people willing to join jihadist groups, finding a safe haven and expanding their frontiers to Southeast-Asia. Extremist groups throughout their existence have had to throw campaigns, propaganda, explicit videos, websites, magazines and subliminal messages in order for them to recruit members; but with the advances in technology and the creation of the internet and social media, their facilities and security loopholes, this task has been made increasingly easier for them. The Internet has also served as a tactical operational tool for terrorists, as far as attacks and strategies go.

ISIS members have increasingly shown interest in Southeast Asia, as a result of losing growth and territory in Iraq and Syria after the Russian military operation in the Syrian conflict targeting jihadist groups in 2015; by the reason of this, they decided to extend their frontier in Southeast Asia in hopes of recruiting new members. Up until now, ISIS members have succeeded in recruiting many new Asian members to join the jihadists through the internet. This problem is not only a national threat in Southeast-Asia, but it also affects various other nations both in the manner of these groups spreading their ideals and operations internationally through various platforms and expanding their borders to more countries.

Cyber recruiting and propaganda

Abu Abdullah al-Maghribi, an ISIS defector aforesaid "The media people are more important than the soldiers, their monthly income is higher, they have better cars, they have the power to encourage those inside to fight and the power to bring more recruits to the Islamic State." (2015). The internet and social media have become an indispensable tool for terrorist groups, either being for propaganda spreading, communication, operation planning, financing or execution. This topic has been discussed before by The United Kingdom, the United States of America, the Russian Federation, etc, and measures such as better surveillance to try and solve it has been implemented, but recent attacks being the bombings in Sri Lanka serve as evidence of these not working. Extremist groups have publicly admitted using social media platforms such as Facebook, Twitter, and Instagram for recruitment purposes, which is alarming considering the amount of youth within these platforms that willingly join them by sympathizing propaganda.

The main way terrorist go unnoticed on social media, is through a large number of bots, which creates a massive communication web in which if an account gets deleted, there is another one ready to replace it, this is a very simple task that has proved to work, although it requires a lot of people to create all of the accounts. A control on all of the accounts is very difficult to achieve if not impossible, and that is what makes the surveillance incompetent. Another commonly used strategy used in social media, is the mass use of popular hashtags that link to accounts that at the same time, link to secure and encrypted sites or apps such as Telegram, WhatsApp, etc. In which they use manipulative techniques to recruit; such techniques include psychological manipulation or empathizing.

It is of relevance to have in mind that, many people join terrorist groups for the economic benefits, as shown in a study made in Somalia released by Mahdi Abdile and released by the European Institute of Peace made in 2018, which showed that 27% of people joining Al-Shabab, were joining them for economic reasons, only 15% joined them for religious reasons and 13% of them were forced to join. The reason why people remain in these groups is only 21% because of the feeling of belonging, and 11% of them stay because of a sense of responsibility, however, economy and fear are also a factor that should be taken in account. Knowing this, we can have a better understanding of the reasons why people join jihadist groups leading to the opportunity of tracking down specific members as well as to have the possibility of handling the situation inside the zones in which terrorists are focusing for recruitment, such as Southeast-Asia. Tracking down geopolitical problems in this region and combating them, can also result in a decrease of terrorist recruitments.

Cyberterrorism and terrorist sites.

Cyberterrorism is the way terrorists utilize the internet to launch and plan attacks, although it is important to know that most attacks do need physical training to be carried out, that is to say, that terrorists have to be qualified in a physical manner to actively participate in it. The way cyberterrorism works is that people who do not physically participate in the attacks, are in charge of logistic, financing and recruiting as they get paid. Another way cyberterrorism works, to hack electrical grids and security systems, or to spread the virus across social media platforms. Terrorism in social media, despite having a noticeable resemblance to cyberterrorism, is different, because terrorism on social media is defined as the set of security threats, activities, and posts related to terrorism being spread by extremist organizations, and does not have a focus on specific tactics or operations used by terrorists. On the other hand, cyberterrorism is the exact way in which terrorist groups carry out their operations making use of the internet.

According to Haifa University, the statistic of extremist sites has exponentially increased in the last decade, from less than 100 sites to more than 4,800. Terrorist sites, are not only those in which recruitment takes place, but those who support and spread extremist messages, showcasing terrorist acts, operations, tutorials, messages, etc. Professor John Arquilla from the Naval Postgraduate school said that “The greatest advantage [Of the Internet] is stealth” and that “Terrorists swim in an ocean of bits and bytes” meaning they have developed numerous sophisticated encryption tools that make the Internet an efficient mean of correspondence. These include steganography and “dead dropping”. Money laundering and other means have eased the recruitment and funding of the pages and the attacks, making it so easy that the transactions can be easily made by PayPal. This issue will get increasingly worse by 2022, when the estimated number of internet users will be over six billion people.

Actions previously taken

Europe has already taken measures regarding this topic, which have worked when first implemented by showing a decrease in terrorist attacks and recruiting, but have not ceased the problem. Implementations of debate forums between governments were made in 2014, in hopes of communication-solving this topic; what this achieved, is that content shifted from being flagged to the immediate detection and elimination of terrorist images, videos, and content. Also, several referral mechanisms aimed at the objective of finding and deleting extremist content have been implemented, they have worked, but there are still numerous websites that don't count with these mechanisms.

Sites that have politics which enable terrorists to securely share information are key to these groups. Having the knowledge of this, many governments have banned sites such as Telegram and demanded backdoor access to their information, however, there still exist lots of encrypted apps. The existence of terrorist online magazines has also being the main link between terrorists and their recruits; these magazines contain interviews, dangerous "do it yourself" sections, violent imagery glorifying their cause, etc. There are several hackers such as Anonymous working on peacekeeping through social media seeking to eradicate extremist groups from the internet, as they work on prevailing democratic ideals, and consider terrorism as a threat to democracy.

Cybersecurity

According to the National Academies Press, the cyberspace is "the set of all computer-communication networks" and "A mayor technology-enabled medium providing means of passage, the locus of objects of value, and parts of the control and management systems for critical processes and infrastructure" (2007). The internet is the largest cyberspace there is, making tracking of everything a very difficult task; to achieve this, every site and application would have to have a perfect software and programing security to keep safe information and discard norm-inflicting content. The mean of passage that the internet has, is a gateway for all types of content that people want to share. The internet is also a medium for important processes to occur, which may put them in risk, such as bank movements, telecommunications, transportation, energy distribution, public health, etc.

As longs as the apps or websites published on the internet are not encrypted, any user can have access to them. The accessibility and lack of software security in a lot of internet-controlled websites made by banks or other important and prestigious organizations and companies, lead to cyber-attacks linked to terrorism and may end up in the funding or recruitment of it. Many companies and banks like the Guaranty Trust Bank (2018) have already had issues with money laundering and terrorist activity, facing lawsuits and legal repercussions. This is why important websites have started to make conscience about the situation and have started taking action countering terrorism.

Some security services, such as Atlas (2017), have implemented policies and measures to counter terrorism on the internet. The measures taken, include both preventive and possible corrective actions in case the filters do not work as expected. A culture of vigilance and awareness is exhorted. Another issue resulting from cyberterrorism is cybercrime and espionage as well as identity theft (occurring every three seconds on average). Cybercrime and espionage occur when an electronic device does not count with a sophisticated security package and becomes infected. Ransomware is a very cheap and easy way of providing terrorist groups with financing.

Measures, such as a National Cyber Security Police by the Atlas UK Security Services, were created to ensure cybersecurity; its objectives include creating a secure cyber ecosystem, an assurance framework and regulatory frameworks, creating mechanisms to detect threats as well as to respond to them and warn about them. This Police promotes the research and development of cybersecurity, reducing supply chains, creating cybersecurity awareness as well as Public-Private partnerships. What this Security Police is seeking for, is that governments invest more infrastructure and time into cybersecurity to better communication between the government and its cybersecurity organizations as well as the industries that develop certain software which might help solving cyberterrorism and other security issues.

Measures to be implemented

To think and implement measures to better cybersecurity, the challenges of this must be considered, resulting in better thinking through of the resolving possibilities revolving this issue. Cybersecurity challenges include its impossibility to reach its fullest potential for reasons such as its inherent and nonremovable vulnerabilities and loopholes, its infinite entry points and development of new encrypted applications and websites each day, the absence of critical massive operations replacing the individual Computer Network Defense techniques, the attack to technology outpacing defense technology, and Nation States, as individuals at a peer level, all capable of waging attacks.

Every smartphone or electronic device sold must count with financed referral mechanisms as well as developing machine learning tools powered by companies with an Artificial Intelligence (AI) such as Google as a preventive measure to counter extremism on the internet and block content before it is published, as well as the necessary software implemented to give information to whichever organization might help. Webmasters must be detected, criminalized and stopped with financial and political international support agreed under the United Nations Security Council´s supervision. Encrypted apps´ security and information sent must be reinforced. These measures shall be taken dispersedly, due to the possible risk of losing a lot of information about how terrorist groups work and their patterns.

Referencias

1. Abdile, M. (2019). Why do people join terrorist organisations? Retrieved on June the 1st 2019, from European Institute of Peace. Web. <http://eip.org/en/news-events/why-do-people-join-terrorist-organisations>

2. Aggrawal, N. (2019). The urgent need to counter terrorism on the internet. Retrieved on June the 5th 2019, from Observer Research Foundation. Web. https://www.orfonline.org/expert-speak/the-urgent-need-to-counter-terrorism-on-the-internet-51381/

3. Atlas UK Services. (2017). Atlas UK Security Services LTD. Retrieved on June the 27th 2019, from Atlas UK Security Services. Web. https://atlas-security.s3.amazonaws.com/assets/21d3ccd88a34e0096746171a0f431b2f0419c4a8/atlas_uk_terrorism_policy_procedures.original.pdf

4. Goodman, S. (2007). 5 Cyberterrorism and Security Measures. Retrieved on July the 4th 2019, from The National Academic Press. Web. https://www.nap.edu/read/11848/chapter/6

5. Harvey, D. (2015). How Islamic State extremists use social media to recruit. Retrieved on June the 6th 2019, from BBC. Web. http://www.bbc.co.uk/newsbeat/article/31574846/how-islamic-state-extremists-use-social-media-to-recruit

6. India TV News Desk. (2016). 15 strict measures taken by government to prevent terrorist attacks. Retrieved on July 4th 2019, from India TV. Web. https://www.indiatvnews.com/news/india-15-strict-measures-taken-by-government-to-prevent-terrorist-attacks-341254

7. M, B. (2018). Why Are So Many Countries Banning Telegram?. Retrieved on June the 1st 2019, from Dogtown Media. Web. https://www.dogtownmedia.com/many-countries-banning-telegram/

8. Operation250. (n.d). How Terrorists Use the Internet. Retrieved on June the 1st 2019, from Operation250. Web. https://www.operation250.org/how-terrorists-use-the-internet/

9. Richards, I and Wood, M. (2018). Hacktivists against Terrorism: A Cultural Criminological Analysis of Anonymous' Anti- IS Campaigns. Retrieved on June the

6th 2019, from Open Access. Web. http://www.cybercrimejournal.com/Richards&WoodVol12Issue1IJCC2018.pdf

10. Saini, R. (2018). Cyber Espionage and Terrorism. Retrieved on June the 27th 2019, from Unacademy. Web. https://unacademy.com/lesson/national-policies-and-framework-for-cyber-security/TFXM6B0X

11. United Nations. (2012). The Use of the Internet for Terrorist Purposes. Retrieved on July the 4th 2019, from United Nations Office on Drugs and Crime. Web. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

12. Tuwray, T. (2018). GT Bank Linked to Money Laundering, Terrorism? Retrieved on July the 4th 2019, from Business Day. Web. http://www.businessdayliberia.com/2018/07/17/gt-bank-linked-to-money-laundering-terrorism/

B

Backdoor access: Using indirect or secret means to achieve access.

C

Correspondence: A connection or communication between two things.

D

Defector: A person who leaves a political party, country, etc. to join another that is considered to be an enemy.

E

Electrical grids: A number of computers that are linked together using the internet so they can share power, data, etc.

Encrypted: Information put in a special code, especially in order to prevent people from looking at it without authority.

F

Framework: The structure of a particular system.

G

Geopolitical: Connected with the political relations between countries and groups of countries in the world or with the study of these relations.

J

Jihad: Holy war fought by Muslims to defend Islam.

L

Locus: The exact place where something happens or which is thought to be the centre of something.

Loophole: A mistake in the way a law, contract, etc. has been written which enables people to legally avoid doing something that the law, contract, etc. had intended them to do.

M

Money laundering: The crime of moving money that has been obtained illegally into foreign bank accounts or legal businesses so that it is difficult for people to know where it came from.

R

Ransomware: A type of software that is designed to block access to a computer system until a sum of money is paid. **Referral:** The act of sending someone who needs professional help to a person or place that can provide it.

S

Safe haven: A place where an individual can go to be safe from danger and attacks.
Stealth: The fact of doing something in a secret or quiet way.
Steganography: The act of concealing a file, message, image, or video within another file, message, image or video.
Stronghold: An area in which there is a lot of support for a particular belief or group of people, especially a political party.
Supply chains: The series of processes involved in the production and supply of goods, from when they are first made, grown, etc. until they are bought or used.

W

Webmaster: A person who is responsible for particular pages of information on the World Wide Web.

Topic B

Measures to prevent terrorism funding, focusing on money-laundering within banks in hopes of weakening their economy causing attacks to progressively slow down

By: Nuria Vidal Castillo

Introduction

The Islamic State of Iraq and Syria is a militant jihadist group founded by Abu Musab al-Zarqawi considered terrorist by the United Nations in 2003. It has committed severe felonies including kidnapping for ransom, extremist acts and attacks, money laundering, etc. The Pricer claims that the Islamic State of Iraq and Syria has a economic capital of over two billion dollars raised mainly for future attacks and weaponry (2014). Terrorist attacks need financing to be sustained, and a lot of the times, these attacks cost around five hundred dollars or less, because many of the supplies utilized are low cost materials that trained terrorists themselves turn into deathly weapons.

Terrorist groups like ISIS and Al-Qaeda have the need for materials such as weapons, equipment, supplies, transportation, etc to attack; to obtain them, they need capital. Hundreds of millions of dollars end up destined for terrorism a year. This topic has been previously debated in the General Assembly (2005), the Counter-Terrorism Committee (2005), the Financial Action Task Force, the International Monetary Fund, etc., but the resolutions planted, did not have the expected results, and that is why this topic needs to be furthermore investigated and debated to find viable solutions. Efforts to weaken this problem have been made for many years, but the money laundering persist.

Money-laundering

The International Compliance Association is a professional membership and awarding body which has made numerous efforts to counter money-laundering by qualifying people to work on financial crime detection, prevention and action. It defines money-laundering as the process by which criminals disguise the original ownership and control of money and the proceeds of criminal conduct by making such proceeds appear to have delivered from a legitimate source. Hundreds of millions of criminal money-laundering proceeds are made annually; and large amount of them, are destined to terrorism. An example of money laundering is when ransom money is deposited into a bank. The amount of money laundered annually can equal Spain's economy (Finantial Action Task Force, 2009).

Not all laundering is illegal, it is only considered illegal when the proceeds come from crimes, such as extremism, kidnapping for ransom, drug trafficking, corruption, bribery, plunder, malversation, car theft, robbery and extortion, piracy, theft, swindling, smuggling, hijacking, terrorism financing, etc. Money-laundering can be made through foreign exchange dealers, pawnshops, money changers, remittance companies, securities dealers, brokers, investment houses, mutual funds, etc. The purchase of Real Estate and the gambling in casinos with “dirty money” may also be considered money-laundering. The Counter-Terrorism Committee has the obligation of detecting and criminalizing money-laundering affiliated to terrorism, terrorism is penalized apart from financial felonies.

Suspicious transactions (where a lot of money is transacted, around P500,000) must always be consulted with the banks before made. Suspicious transactions may include: No underlying legal or trade obligation, purpose or economic justification, the client is not properly identified, the amount transacted is not commensurate to the client's capacity, etc. Normally, to make money-laundering a successful process, it follows three basic steps. The first step, often referred to as “placement” consists in criminals introducing illegal funds into the financing system (banks) to make the money seem as it is not linked to unlawful activities; to make this process seem legal, often times, criminals break the amount apart into smaller money quantities so it is not a suspicious transaction. The second step, is called “layering”, and consists of making the money go through various transactions to completely disguise the source, and criminals may mask these transactions by using the money for payments of goods and services giving them a legitimate appearance. The third step, called “integration” is where criminals can finally receive and spend the money which has been “cleaned” from its illegal source through all of the previous steps and transactions.

Terrorism financing and money laundering

The way terrorist groups work their financing is simple, first, they get capital to sustain organizations and their infrastructure, then, they transfer the funds to carry out any terrorist attack. The raise of funds may be bot in illicit or legal forms. Extremist fundings are made in many different ways, although the main way is by affiliating with corrupt banks or committing fraud to them, as seen in the ING Belgium bank prior to the creation of the Ultimate Beneficial Owner Identification Form which prevents the funding of terrorism by fulfilling a number of client identification obligations, or with the HSBC bank, has publicly admitted to destin hundreds of millions of dollars to the financing of terrorism in more than one occasion. Court filings have proof that ever since 2006, more than a dozen banks have dealt with criminal offenses. Money laundering is one of the biggest problems, and the supporting of these acts from banks has got to stop in order to decrease terrorist funds.

When an illicit funding of terrorism is made, it usually leaves a trace behind. It is important to trace that trail after an extremist attack occurs, in order to learn and prevent them further on. The Federal Bureau of Investigation (FBI) has formed a Terrorist Financing Operation Section (TFOS) which conducts the full financing analysis of terrorist suspects and and their financial support structures. TFOS is conformed by a large amount of people professionally prepared by the FBI which has full access to every suspect´s information, background and data, making the efforts to prevent and stop money laundering from the source easier.

Terrorists need to carry out a series of steps when laundering money, which need to accomplish three things, to erase the link between the crime and the money, erase the link between the money and its new owner, and finally to shelter the incomes from possible finding and confiscation. First of all, they have to enter the money to a banking system; this action has become more difficult for them due to banks reinforcing their security and reporting every suspicious movement; but fraudulent banking systems and contacts make it possible for extremists to still introduce illicit money. Misleading financial operations make it so that the funds enter the financing system appearing as legitimate and legal using offshore mechanisms and financial havens. After these steps, terrorists consume an amount of the money in luxury items with a high cost, legal services, investments, businesses which become money laundering machines such as casinos, hotels, etc.

Serious strategies to combat money laundering need to be implemented such as prevention by identifying commonly money laundering used businesses and processes and placing more limitations on those. Detecting money-laundering operations through legislative operations, reporting suspicions and implementing specialized investigative measures including full access to computing mechanisms in banks and their transactions, commercial banking information, etc.

Financial Action Task Force (FATF)

The Financial Action Task Force is an inter-governmental body, established by the Ministers of its Members jurisdictions in July 1989 in Paris, France. It was first made as a measure to combat money laundering. Its current objective is set standards and promote effective implementation of legal, regulatory and operational measures for combating money-laundering and terrorist financing amongst others which threaten the financial system. The FATF defines itself as a "policy-making body" which works to generate the necessary political will to combat international financing threats.

It has created a series of recommendations called "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations" which are now recognized as the international standard for the combating of money-laundering and the financing of terrorism and proliferation of weapons of mass destruction. The recommendations were last revised in 2012 to make sure they remain relevant and updated. The FATF has a decision-making body which meets three times per year.

The Financial Action Task Force, is a really big tool for money-laundering related topics, due to its governmental facilities and opportunities and its focus on money-laundering and terrorism financing. It has taken part in a lot of major United Nations Committees decisions and resolutions, such as the United Nations Security Council's resolution 1373 in 2001. The FATF has also made various recommendations on money-laundering criminalizing, which one of the Counter-Terrorism Committee´s first priority and obligation.

Difficulties on defeating money-laundering

Eduardo Arbizu, the head of the Global Head of Supervisor, Regulation and Compliance at BBVA, says that anti-money laundering tasks are easy to define, however, carry it out has become increasingly more difficult over the years. Many times, the urge to detect illicit money and prevent it from being laundered in banks has been debated. The BBVA´s Global Head of Supervisors, Regulation and Compliance aforesaid that criminal activity has increasingly become more complex by the day, and that is why money laundering has pivoted and become a top priority in any banking system. The financing system is the medium and filter in which money flows, which is why it has a great advantage as far as the identification of illicit money goes.

Accordingly to Eduardo Arbizu, there are six major challenges in countering money laundering, the first one being the international footprint which is where banks have to develop an international anti-money laundering vision, setting international standard preventive and active measures for money-laundering, assuring that money laundering is a global issue. Another challenge is supervisory pressure, meaning that putting so much pressure on people to supervise that excessively, therefore discouraging activities that entail higher money laundering risks, also known as "derisking" can have undesired side effects such as refraining from offering correspondent banking services in developing countries affecting their economies.

The maximizing and effectiveness of institutions is making money laundering exponentially grow and become more complex due to the easy-fooling banking security systems forcing terrorist groups to reinforce their methods and be exponentially more dangerous and advanced. The technological challenge is another impedition and opportunity to better, because artificial intelligence and should be implemented into improve security and prevent money laundering and other financial problems. Recognizing talent and training professionals to take over and be able to innovate and deal with problems in a more educated way. Finally, raising awareness in society about mutual collaboration between banks and users needs to be done.

Previously taken actions

Previous measures have been taken to deal with terrorism financing, such as the Counter-Terrorism Committee creating The Counter-Terrorism Implementation Task Force (CTITF) in 2009. A Security Council resolution 1373 which urges the need to suppress the financing of terrorism, amongst many others, but international cooperation is of extreme relevance in these situations, and with technology evolving, this topic has turned harder to convey with was made in 2001. An International Convention for the Suppression of the Financing of Terrorism adopted by the General Assembly (1999) in which a resolution paper was achieved a resolution paper counting with 28 articles. The united Nations Office on Drugs and Crime along with the International Monetary Fund made a model legislation on money laundering and financing of terrorism with 6 articles.

The Security Council's resolution 1373 purposes include the prevention and suppression of terrorism and its acts, the criminalization of money laundering and terrorism financing, freezing and confiscation of terrorist assets, and preventive measures to be taken by financial institutions such as: The Financial Action Task Force (FATF) recommendation 13 addressing the reporting of suspicious transactions and suppliance. The bank for International Settlements made an article on the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (1988).

Measures to be implemented

To solve this issue, these form of terrorism financing must be addressed in a formal debate with the 15 members of the Security Council Committee. It is of extreme relevance to address the Counter-Terrorism Implementation Task Force to be able to reinforce it and remodel it accordingly. Extreme surveillance on banks throughout the world is required, as well as a report on any suspicious movements, which have to be sent to the Counter-Terrorism Committee to freeze the accounts and judge people in question along with their legal consequences. International Internet security must be reenhanced and exhorts the International Criminal Police Organization (INTERPOL) to take part in this process. In sights of The Ultimate Beneficial Owner Identification Form working, all banks are required to have this form and utilize it on every movement. Any affiliation with terrorism identified within any bank, must be criminalized immediately and the bank must be in constant probation and surveillance.

Referencias

1. Bank for International Settlements. (1988). Prevention of criminal use of the banking system for the purpose of money-laundering. Retrieved on July the 10th 2019, from Bank for International Settlements. W eb. <https://www.bis.org/publ/bcbsc137.pdf>
2. Cabirta, A. (2019). Anti-money laundering challenges in the financial sector. Retrieved on July the 18th 2019, from BBVA. Web. <https://www.bbva.com/en/anti-money-laundering-challenges-in-the-financial-sector/>
3. Counter-Terrorism Implementation Task Force. (2009). Tackling The Financing of Terrorism. Retrieved on June the 2nd 2019, from Counter-Terrorism Implementation Task Force. Web. <https://www.un.org/en/terrorism/ctitf/pdfs/ctitf_financing_eng_final.pdf>
4. Financial Action Task Force. What we do. Retrieved on July the 10th 2019, from Financial Action Task Force. Web. <https://www.fatf-gafi.org/about/whatwedo/>
5. ING. (n.d). Ultimate Owner Identification Form (As well as the identification of any "politically exposed persons" who are living outside Belgium). Retrieved on June the 2nd 2019, from ING. Web. <http://www.ing.be/Assets/content/groups/internet/@public/@internet/@ingbe/documents/po rtalcontent/452674_en.pdf>
6. International Compliance Association. (n.d). What is money laundering? Retrieved on July the 10th 2019, from International Compliance Association. Web. <https://www.int-comp.org/careers/a-career-in-aml/what-is-money-laundering/>
7. Legislation.gov. (2017). The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Retrieved on June the 10th 2019, from Legislation.gov. Web. <http://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi_20170692_en.pdf >
8. Mazur, R. (2013). How to Halt the Terrorist Money Train. Retrieved on June the 10th 2019, from The New York Times. Web. <https://www.nytimes.com/2013/01/03/opinion/how-bankers-help-drug-traffickers-and-terror ists.html >
9. Morehart, M. (2004). Terrorist Financing and Money Laundering Investigation. Retrieved on July the 18th, 2019, fromTheFederalBureauofinvestigation.Web. <

https://archives.fbi.gov/archives/news/testimony/terrorist-financing-and-money-laundering-i nvestigations-who-investigates-and-how-effective-are-they>

10. Panganiban, A. (2016). Money Laundering 101. Retrieved on July the 10th 2019, from Inquirer Opinion. Web. <https://opinion.inquirer.net/94432/money-laundering-101>

11. Petkovic, N. (2011). Terrorism in other Countries: Funding, Where Terrorist Organizations get their Money. Retrieved on June the 2nd 2019, from Blogspot. Web. <https://terrorismintheworld1.blogspot.com/2011/04/funding-where-terrorist-organizations.ht ml >

12. Reyes, A. (2012). Kidnapping for Ransom: The Growing Terrorist Financing Challenge. Retrieved on June the 6th 2019, from U.S Department of the Treasury. Web. <https://www.treasury.gov/connect/blog/Pages/kfr-cohen-europe.aspx>

13. ThePricer. (2014). How Much Does A Terrorist Attack Cost? Retrieved on July the 10th 2019, from ThePricer. Web. <https://www.thepricer.org/how-much-does-a-terrorist-attack-cost/>

14. Thony, J. (n.d). Money Laundering and Terrorism Financing: An Overview. Retrieved on July the 18th, 2019, from InternationalMonetaryFund.Web. <https://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf>

15. United Nations. (n.d). FATF Recommendation 13: Reporting of suspicious transactions and compliance. Retrieved on July the 10th 2019, from United Nations. Web. <https://www.un.org/sc/ctc/wp-content/uploads/2016/03/fatf-rec13.pdf>

16. United Nations. (1999). International Convention for the Suppression of the Financing of Terrorism. Retrieved on July the 10th 2019, from United Nations. Web. <https://www.un.org/law/cod/finterr.htm>

17. United Nations. (2001). United Nations Security Council resolution 1373 (2001). Retrieved on July the 10th 2019, from UnitedNations.Web. <https://www.un.org/sc/ctc/resources/databases/recommended-international-practices-codes- and-standards/united-nations-security-council-resolution-1373-2001/>

18. United Nations Office on Drugs and Crime. (2011). Illicit money: how much is out there? Retrieved on July the 18th, 2019, from United Nations Office on Drugs and

Crime. Web. <https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-t here.html>

19. United Nations Office on Drugs and Crime. (2005). Model legislation on money laudering and financing of terrorism. Retrieved on July the 10th 2019, from United Nations Office on Drugs and Crime. Web. <https://www.unodc.org/documents/money-laundering/2005%20UNODC%20and%20IMF% 20Model%20Legislation.pdf >

20. United Nations Security Council Counter-Terrorism Committee. (n.d). Terrorism Financing. Retrieved on June the 2nd 2019, from United Nations Security Council Counter-Terrorism Committee. Web. <https://www.un.org/sc/ctc/focus-areas/financing-of-terrorism/>

21. Watson, A. (2015). Islamic State and the "blood antique" trade. Retrieved on June the 6th 2019, from BBC. Web. <http://www.bbc.com/culture/story/20150402-is-and-the-blood-antique-trade>

22. Williams-Grut, O. (2015). How ISIS and Al Qaeda make their money. Retrieved on June the 2nd 2019, from Business Insider. Web. <https://www.businessinsider.com/how-isis-and-al-qaeda-make-their-money-2015-12#6-sca mming-banks-1>

A

Affiliate: Officially attach or connect (a subsidiary group or person) to an organization.

F

Felony: The series of processes involved in the production
and supply of
goods, from when they are first made, grown, etc. until they are bought or used.

M

Malversation: Corrupt behavior in a position of trust, especially in public office.

P

Pawn Shop: A shop where loans are made with personal property as security.

Plunder: Steal goods from a place or person, normally force and in a time of war or civil disorder.

Proliferation: Rapid increase in the amount of something.

R

Ransom: A sum of money demanded for the release of a captive.

Refrain: To stop oneself from doing something.

Remittance: A sum of money made in payment or as a gift.

S

Swindle: Use deception to deprive (someone) of money possessions.