E-ISSN: 2664-603X
P-ISSN: 2664-6021
IJPSG 2022; 4(1): 06-09
www.journalofpoliticalscience.com
Received: 02-11-2021
Accepted: 09-12-2021

Zharama M Llarena
BA Political Science Student, Department of Politics, Justice, Law, and Philosophy University of North Alabama, USA

Corresponding Author:
Zharama M Llarena
BA Political Science Student, Department of Politics, Justice, Law, and Philosophy University of North Alabama, USA

Code development of regulatory technology for legitimacy of cybersecurity adjudication

Zharama M Llarena

DOI: https://doi.org/10.33545/26646021.2022.v4.i1a.126

Abstract
Artificial Intelligence (AI) on cybersecurity is designed to control financial transactions and agreements worldwide. It is an innovative regulatory tool architecturally networked to combat cyber threats and attacks in various degrees of war and crime perpetration from various banking industries and its corresponding government authority functions with implementing arms for execution of monitoring, reporting, and compliance. Regulatory Technology (RegTech) is an AI tool used by treasury departments and institutions, both local and private, for tracking malicious threats possible for money laundering and terrorism financing concealed in various settlements around the world. However, cybersecurity decisions need conformity in regulations and proceedings that it aims to engineer code development involving attacks under Regulatory Technology usage for administrative functions in favor of the financial intelligence authorities for combating and resolving issues on cyberwar. Therefore, political adjudication is a developing means of resolving gaps and optimizing judicial process principles within the policy function of financial intelligence. Hence, international laws and its accompanied policies must be globally harmonized in terms of federal and transnational tracking of financial flows of assets.

Keywords: Cybersecurity, terrorism, cybercrime, money laundering, political adjudication

Introduction
The context of banking industries has dramatically improved for 20 years subsequent to 2008 predicaments on financial flows. The new monetary policies had a remarkable impact for processing the volume and complexity of several banking activities focusing on balance sheet of capital management, trade finance, profitability, lending, as well as liquidity. Hence, the conformity of banks to comply with their supplementary requirements made a tremendous effect on the wider scope of banking landscape.

The increment of regulatory reporting after its worldwide banking crisis had a significant impact in terms of its processed volume. The conventional reporting of several financial firms gained complexity as reflected for its vast consumed time. The length of time spent is divided with the number of reporting for submission of organizational regulatory reports and the volume of necessary supplements for compliance expansion. Hence, there is an observed problem in reporting documentation as its compliance time in including varying requests is found to be hard to manage.

The policy advances in regulatory and compliance is described to be an immense measurement in terms of length in reading time for understanding the focus of US banking regulations. In comparison with 2017 statistical information, a person can manage to understand the entire and pertinent regulatory references in 3 years of time at an approximate speed of 5700h or 300 words per minute with allotted weekend rests. Hence, if an individual can finish reading all works of Shakespeare in an estimated time of 50h as much as he would understand the whole Bible at faster time of 45h, his Shakespeare readings compared to US policies on regulatory and compliance can take at a rate of 115 times more [1].

Compliance is vital for banking firms not only from an economical resources' point of view but also for the reason of market stability. Regulatory documents are essential for ensuring customer protection, hence, a preventive measure, and its establishment affects the wealth of the nation as well as the foreign economy for an entire perspective. Furthermore, it is an advantage for Central Banks to utilize these regulations as these policies would result to probability reduction of bailing banks and specification of its potential issues would impede a broader impact on market economy. The reason for banking institutions' strict conformity

with policies is due to avoidance of reputational taint, implemented sanctions, and investor's confidence loss resulting to punishments such as trading suspension and banking license revocation [1].

There is an obligation for the augmented digitization in the financial firms due to intervention of novel technologies and technology industries in the banking sector. Industries and systems of financial technology (FinTech) have initiated to develop several financial market areas. Based from Gabor and Brooks (2017), FinTech firms and applications have significantly influenced specific domains of funding platforms, financing protocols, and payment systems. Financial institutions (FIs) focused their vital concerns on management of activities pertaining to risk and compliance, thus, Institute of International Finance referred regulatory technology (RegTech) as their novel technological solutions. At a recent assessment with other contemporary designs, RegTech is considered to be at an early phase of advancement.

The Institute of International Finance described regulatory technology as the utilization solution of novel innovation to answer problems effectively and efficiently on regulatory and compliance documents. Furthermore, in 2017, Arner *et al*., defined RegTech as an IT innovation utilization in a controlled landscape specialized to monitor, report, and comply with financial requirements. Hence, it is an innovative solution optimized within business context comprising of industries or organizations aiming to aid financial firms in their regulatory problem transactions. A crucial advantage of implementing RegTech is not merely for IT application of risk management operations, rather, its technology is integrated for solution assistance [2].

The United States started to hold seriously with apparent equipped resources activities found to be suspicious in conformity of cybersecurity. During 2009, the Defense Secretary ordered a Cyber Command establishment in their Executive Branch Department in order for the foreign experts to deliberate and formulate solutions on cyber-attacks known as Tallinn Manual which discusses the application of international law regulations in details, and Tallinn Manual 2.0 is a sequel of the former one explaining the principles of international law that can applied during peacetime of cyber functions. However, these group of international experts did not have the opportunity to establish a formal distinctive line separating cyber operations perpetrating a hostile armed attacks and offenses inadequate to meet a grave weapon destruction, or unable to divide situations between a heavy mass impairment and those approaches that can be considered within law enforcement concerns

There are issues that can be raised for the enforcement of civil and federal security against cybercrimes. There are numerous determinants influencing the appropriate susceptibility of the United States to be damaged from suspicious cyber movements. During 2018, DHS Secretary Kirstjen Nielsen announced that the usage of digital technology in this modern era can endanger our lives as threats can be specified originating from enemy states, terrorists, and foreign criminals, in addition to existing criminals and terrorists within their jurisdiction. Facing several threats that have increased confusions between foreign crime and armed attack, the U.S. government combats the challenges their federal security is encountering at a relevant cost both in physical and cyber domains. The law enforcement implements a displacement approach for a weapon conflict framework conveying outcomes for institutional conceptual network system, law authorities, and money distribution. Hence, a militarized solution may lead distinctively to foreign cyber attacks implicating that domestic officers of law enforcement is obliged to abandon insufficient training, resources, and support to ascertain, prevent, and sanction criminals. There is a great demand for better solutions coming from law enforcement coordination and its money allocation to implicate a comparable urgency for maintaining the focused monitoring crucial for elemental crimes of most suspicious cyber movements.

The ambiguity as well as difficulty to extricate and de-risk armed and civilian operations corresponds to the volume of weapon attack in cyberspace in suspicion of cyber movements. Within the cyberwar design, the Defense Department introduced a policy concerning protection from interruption or impediment of detected suspicious cyber movements, with the inclusion of crime problems below the level of weapon conflict. Concerning law implementation, Justice Department has engaged cybercrime operations for elemental illustration leading to identification, deterrence, and sanction of suspicious cyber perpetrators, as well as their accomplices, who aimed to attack private industries [3].

Terrorism is a worldwide chaos starting from World War II that spawned a significant impact across countries around the globe. It is a notorious destruction of displaced tranquility resulting to killing of many civilians including women and their children. Its main design intends to destabilize the national serenity in Islamic countries to generate phenomenon in Western chaos. Hence, foreign communities must deal and handle this chaotic violence resulting to cruel impacts in order to protect their nation from repeated terrorisms.

Global terrorism corresponds to financial activities allocated to plot a massive destruction through a nation and it is apparent that worldwide chaos would need an enormous monetary capacity. Foreign communities specified that some organizations were able to scheme these chaotic attacks lurking in financial activities of money laundering and terrorism financing. Hence, these international experts from various organizations formulated regional, bilateral, and foreign agreements, through conventions and resolutions, to detect and combat financing of terrorism resulting to money laundering impediment [4]. Due to inadequacy in conformity of implemented rules and regulations, as well as the relevance of the introduced technology, this paper aims to develop a code for administrative policy as an authoritative function resolving issues on cybercrime and terrorism attacks in alignment with political adjudication.

Methods

Money laundering is a concealment act to further undergo satisfaction of criminal intent. This misrepresentation performance needs to be addressed crucially as it allows perpetrators to take advantage of their iniquitous movements without getting caught in public. During the G-7 summit in Paris of July 1989, financial action task force (FATF) was created as an independent body acting between governments designed to develop and advocate protective policies of the global banking system in opposition to money laundering and terrorism financing. In 1996, FATF established an international standard for anti-money laundering with 130

countries to support the Forty Recommendations. In October 2001, subsequent to the World Trade Center terrorism attack, the FATF formulated the Eight Special Recommendations for combating financing on terrorism as complementary expansion of its official order to resolve encountered issues in terrorism financing. In October 2004, an additional Special Recommendation was added to the existing measures of anti-money laundering (AML). Furthermore, the 40 + 9 recommendations were revised in 2012 focusing on risk-based approach and integrated comprehensively supplementary statements on anti-money laundering, money proliferation and anti-terrorism [5].

Regulatory technology (RegTech) has shown vitally to increase its agreements and its demand has illustrated advanced threshold for banking regulators since this technological solution has an enhanced capacity for supervision and regulation of compliance. Traditionally, the U.S. banking institutions spent an approximate of US25B per annum for their human resources and IT services designed for compliance of anti-money laundering (AML). In the spawn of regulatory technology (RegTech), there is an augmenting fast development in the technology provision complying its solutions concerning expenditures, monitoring, facilitating better evaluation and lowering anticipated risks. According to Zabelina *et al*. (2018), this innovative tool is designed to assist organizational compliance maintaining to keep up-to-date the continuing modification of requirements according to legal principles, hence, created to provide security to banking firms for reliability, safety, and affordability of solutions resulting to increment of their efficient utilization. Thus, it provides combating technologies against money laundering activities in all detailed means such as collecting intricate and dispersed data from various origins that manual search is difficult for regulatory compliance. Therefore, RegTech is vital for the provision of AML risk information, client data through onboarding, filtering, and tracking, and data analytics for clients [6].

Through global efforts, processing of legislation from regional jurisdiction to federal execution and employment had generated an up-to-date regulatory movement. The European Union (EU) formulated EU Regulation in order to apply criminal principles and information technology framework in conformity with AML regulations in varied levels and landscapes. The Financial Action Task Force (FATF), the European Council, the United Nations, and financial organizations have complementary movements facilitated in international conventions for equivalent transfers of authorities [7]. Foreign terrorism is found to have three fundamental elements:

1. Seeming beyond the strategic range of economic, political, or religious attacks (famous theater)
2. Broad fundamental support that guarantees sudden global spread (cyberspace)
3. Unlimited concept of the adversary in targeting his goal inflicting maximum damage within short duration of time (territories of USA) [8]

The theoretical foundation of compliance principles is based on a common ground of variables featuring the elemental behavior of the state. The prominence of soft compliance in foreign law and its relations is vastly argued on its lawfully non-binding standards in consideration of their threshold to sustain global tranquility according to its theoretical perception, controlled prescription, and practical demonstration. There is common subject for discourse in foreign law and international relations known as soft law that plays a crucial part in the foreign legal framework based on its characterized standard for compliance of requirements. In any rate of binding and non- binding effect, there is lack of definite distinction that would separate the insights perceived with soft law and its association to compliance, hence, scholastically agreed to be dichotomous for strategic compliance and not to reduce the relevance of legal standard. International cooperation on soft law compliance under AML/CFT creates a demand for a framework transition transposing the dichotomy focus to adapt its legal standard structure based on information, precision or monitoring, entrustment, monitoring, and punishments conveying global order and protection [9].

Discussion

Hawala is basically defined as the conveyance of money in lack of apparent banking activities, such as traveler's check and countervaluation. Thus, hawala trade is not basically considered to be bilateral as concurrent agreements might be observed with other parties of Istanbul, London, Muscat, Dhaka, etc. Moreover, bundled transactions comprising of thousands or hundreds of agreements consolidated in a month or week course are displaced at several levels for contract settlement.

Throughout several years, the law enforcement of the United States reported that bulk currency smuggling remains to be the biggest and most remarkable threat to access money laundering strategies. In 1998, the US State Department documented the smuggling act of bulk cash across boarders in their International Narcotics Strategy Report as majority of financial flow transactions move through alternative routes. Hence, criminals can indirectly manage to penetrate US banking institutions to proceed with money laundering [10].

In spite the fact that Tallinn Manual 2.0 is formulated to apply international law, there is still a need for further developments between states and countries to promote a share understanding for advocacy of stable foreign relations. Unfortunately, there is lack of appropriate institutions as well as suitable processes to combat cited grievances detected in suspicious cyber movements for fulfillment of their duties and obligations. Furthermore, disagreements had been held in several US jurisdictions as Organization for the Prohibition of Chemical Weapons (OPCW) and International Atomic Energy Agency (IAEA) were monitoring and enforcing compliance based on treaty commitments. As a result, there are associated technical problems being observed in cyber flows since there is insufficient official authorities and no particular system is designed that would particularly resolve issues on suspicious cyber movements and punish perpetrators for accountability solutions [11].

Code development is a political judicialization process in order to treat issues on administrative policies for alignment of organizational goals. Department of Justice has an organized means of resolving issues on cybercrime detection involving money laundering and financing of terrorism. European Law (EU Law) has imposed regulations on banking industries worldwide concerning transactions within their territory and transnational agreements in order to monitor, report, and comply financial flows that are

deemed to be suspicious and subject the found problems and threats to legal settlements. Regulatory Technology (RegTech) is a 2015 innovative tool designed to assess financial movements through artificial intelligence. However, Department of Defense has inadequate ways of implementing necessary laws, whether international, federal or its equivalent, of combating security predicaments on cyberwar. Above cyber threats on observed crime perpetration for cybersecurity, implementation of soft law for money laundering and terrorism financing for application of Regulatory Technology (RegTech) in their Tallinn Manual 2.0 must be aligned with the existing rules and regulations of the Department of Justice in order to harmonize the efficiency of all administrative functions involving government treasuries and banking industries, together with its equivalent, with the common goal of protecting the wealth, economic ties, and security of all nations worldwide.

Conclusion

The financial context of money and other asset transactions are centered in several banking institutions and other treasury departments of their corresponding government with administrative functions to control their existing regulations. Regulatory Technology is an efficient artificial intelligence tool innovated to control and de-risk various flows of assets transacting globally for detecting malicious threats involving money laundering and terrorism financing. The Justice Department has an ideal authoritative power for engineering policies of other executive branches of the government. Cybersecurity is a Regulatory Technology tool integrated in banking industries resulting to protection and surveillance of various asset flows running simultaneously and subsequently for tracking visible attributions of terrorism and characterize its economic impact ranging from various cybercrimes involving money laundering and terrorism financing up to cyberwar. Hence, political Judicialization is essential for developing regulations in the Tallinn Manual 2.0 of Department of Defense. Thus, integration of Regulatory Technology policies into the financial intelligence aspect of Defense Department results to code development for compliance of cybersecurity judicial opinions which is substantial for comparison of international laws, federal statutes, administrative functions and necessary sanctions and punishments for illegal business trades, hence, damaging the economy and security of a nation and other affected territories.

References

1. Solms JV. Integrating Regulatory Technology (RegTech) into the Digital Transformation of a Bank Treasury. Journal of Banking Regulation. 2020;22:152-168.
2. Becker M, Merz K, Buchkremer R. RegTech-The Application of Modern Information Technology in Regulatory Affairs: Areas of Interest in Research and Practice. Intelligent Systems in Accounting, Finance and Management. 2020;27:161-167.
3. Eoyang M, Keitner C. Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity. Journal of National Security Law & Policy. 2021;11(327):327-342.
4. Rabie ZM. Combating the Crime of Money Laundering to Finance Terrorism Study in International Law. International Journal of Asian Social Science. 2018;8(6):265-283.
5. Mei DX, Ye YY, Gao ZG. Literature Review of International Anti-Money Laundering Research: A Scientometrical Perspective. Open Journal of Social Sciences. 2014;2:111-120.
6. Turki M, Hamdan A, Cummings RT, Sarea A, Karolak M, Anasweh M. The Regulatory Technology "RegTech" and Money Laundering Prevention in Islamic and Conventional Banking Industry. Heliyon. 2020;6:1-11.
7. Bergstrom M. The Many Uses of Anti-Money Laundering Regulation – Over Time and into the Future. German Law Journal. 2018;19(5):1149-1167.
8. Schneider F. The (Hidden) Financial Flows of Terrorist and Organized Crime Organizations: A Literature and Some Preliminary Empirical Results. IZA Discussion Paper. 2010;4860:1-42.
9. Beekarry N. The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law. Northwestern Journal of International Law & Business. 2011;31:137-194.
10. Bowers CB. Hawala, Money Laundering, and Terrorism Finance: Micro-Lending as an End to Illicit Remittance. Denver Journal of International Law & Policy. 2009;37(3):379-419.
11. Davis II JS, Boudreaux B, Welburn JW, Aguirre J, Ogletree C, McGovern G. Stateless Attribution: Toward International Accountability in Cyberspace. RAND Corporation. 2017, 1-57.