Vol.12 • 2019 ISSN. 1307 - 9190

Defence Against Terrorism Review

DATR

Struggling with the Financing of Terrorism: Inadequate International Cooperation in Human Trafficking
Bilgin Birlikseven

Methods of Martyrdom: Examining Changing Targeting Patterns in Suicide Attacks Towards Non-Democratic States
Jakob Urda

Ransomware, A Tool and Opportunity for Terrorist Financing and Cyberwarfare
Alan Brill and Eric Thompson

Assessing Legal and Policy Responses to Boko Haram's Terrorism in Nigeria
Dr. Uchenna Jerome Orji

COE-DAT
Centre of Excellence Defence Against Terrorism

Defence Against Terrorism Review - DATR **ISSN 1307- 9190**

DATR is an international peer-reviewed journal that is abstracted and indexed in EBSCO Publishing.

DATR is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT). It is produced for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. It does not represent the opinions or policies of NATO or COE-DAT. The views presented in articles are those of the authors.

Defence Against Terrorism Review - DATR **ISSN 1307 - 9190**

DATR dergisi uluslararası hakemli bir dergidir ve EBSCO Host veritabanı tarafından taranmaktadır.

DATR dergisi Terörizmle Mücadele Mükemmeliyet Merkezi (TMMM)'ne ait bir yayındır. NATO, NATO Üye ülkeleri, NATO Ortaklık Ülkeleri, ilgili özel kuruluşlar ile kamu kurumları ve ilgili kişilerin kullanımı için hazırlanmaktadır.

DATR dergisinde yayınlanan yazılarda bilirtilen fikirler yalnızca yazarına/yazarlarına aittir; TMMM'yi NATO'yu ve NATO'nun fikir ve politikalarını temsil etmez, bağlamaz.

Yayın Sahibi: M.Özgür Tüten
Sorumlu Yazı İşleri Müdürü: Mahmut Erdem
Yayın Türü: Yerel Süreli Yayın
Yayın Şekli: 6 aylık İngilizce

Defence Against Terrorism Review – DATR
(Terörizmle Mücadele Değerlendirme – DATR)
Terörizmle Mücadele Mükemmeliyet Merkezi
(TMMM)

Devlet Mahallesi İnönü Bulvarı
Kirazlıdere Caddesi No:65 06582
Çankaya/ANKARA

Tel: 0 (312) 425 8215
Faks: 0 (312) 425 6489
E-posta: datr@coedat.nato.int

Baskı: Başkent Klişe Matbaacılık
Bayındır 2 Sok. No: 30/E
Kızılay/ANKARA
Tel: 0 (312) 431 54 90

Defence Against Terrorism Review
DATR

Vol. 12, 2019

ISSN. 1307-9190

CONTENT

The Defence Against Terrorism Review (DATR) is calling for papers for coming issues. The DATR focuses on terrorism and counterterrorism. All of the articles sent to DATR undergo a peer-review process before publication. For further information please contact datr@coedat.nato.int

Editor's Note

Dear Defence Against Terrorism Review (DATR) Readers,

The Centre of Excellence-Defence Against Terrorism (COE-DAT) proudly presents 12th Volume of DATR which features four articles on a wide range of aspects of terrorism.

The current issue begins with an article by Bilgin Birlikseven titled *"Struggling with the Financing of Terrorism: Inadequate International Cooperation in Human Trafficking"*. In this article Birlikseven discusses the issue of inadequate international cooperation in the struggle against the financing of terrorism regarding human trafficking. He describes Human Trafficking and explains the Nexus between Human Trafficking and Terrorist Organizations. He handles the crime of human trafficking and the income obtained from this crime in the context of terrorist organizations. The conclusion of this article focuses on the importance of increasing international support, guidance, pressure and sanctions against the countries that offer inadequate cooperation to solve these problems preventing cooperation.

The second article of this issue by Jakob Urda focuses on suicide attacks in Non-Democratic States. This article examines trends surrounding suicide attack targeting. Specifically, it looks at the pattern of terrorist groups targeting states with democratic governments versus states with authoritarian governments. In his article entitled "Methods of Martyrdom: Examining Changing Targeting Patterns in Suicide Attacks towards Non-Democratic States", Urda argues that this longstanding relationship no longer holds true. Today, almost every suicide campaign targets a country which has limited or non-existent political liberty. In this article, Urda uses three decades of Freedom House data to show that democratic institutions are no longer necessarily the primary targets of suicide terrorism, and offers explanations as to why. Autocracies are now the main targets of terrorist groups using suicide attacks.

Alan Brill and Eric Thompson discuss the anti-terrorist and cyberwarfare communities on the potential use of ransomware for funding terrorist or rogue states in the third article of this issue titled "*Ransomware, A Tool and Opportunity for Terrorist Financing and Cyberwarfare*". They suggest that malware and ransomware, currently used to cripple corporations, could also disrupt military and civil government operations, build fear in civilian populations and further the goals of anarchists, adversary nation-states - or terrorist groups. In this article, the authors discuss how ransomware and other types of malware can be repurposed by nation states or terrorists to disrupt military and civil government operations while hiding behind the guise of a credible alternative perpetrator - cybercriminals. The exponential escalation in ransomware payments, which has resulted in a multi-level financial model of providing ransomware and malware as services, is also discussed. New financial resources can be used to train an ever-increasing number of front-line cyber threat actors with the developers safely out of harm's way. More importantly, these services now provide terrorist groups, who would otherwise not possess the technical skill to carry out cybercrime, with a set of weapons that were previously unavailable to them.

In the last article of this issue entitled "Assessing Legal and Policy Responses to Boko Haram's Terrorism in Nigeria", Uchenna Jerome Orji addresses the question whether the establishment of legal and policy measures for countering terrorist activities has effectively contributed in tackling the violent extremist activities of the Boko Haram sect? In order to address this question, Orji adopts as a doctrinal research method to undertake an analytical review of Nigeria's counter terrorism laws and policies. The author examines the efficacy of Nigeria's counter terrorism laws and policies in tackling the terrorist activities of Boko Haram. In so doing, Orji identifies factors that have impeded the effective enforcement of Nigeria's counter terrorism measures in tackling Boko Haram's activities and further proposes responses that can be adopted to improve their enforcement and implementation. The author also recommends a review of the detention powers under

section 27(3) of the Terrorism Prevention (Amendment) Act and the establishment of a justice administration policy that will facilitate the expeditious prosecution of cases involving members of Boko Haram.

As DATR team, we would like to thank all authors and referees for the contributions they have made to this issue and encourage readers to send us comments and suggestions. DATR always welcomes and encourages contributions from experts, civil and military officers as well as academics to send us their best work on defence against terrorism.

Sincerely yours,

Uğur Güngör
Editor-in-Chief

DATR, 2019; 12 : 7-27

ISSN 1307 - 9190

Struggling with the Financing of Terrorism: Inadequate International Cooperation in Human Trafficking

Bilgin Birlikseven[1]

Abstract: *Human trafficking comes to the fore as a major and particularly heinous crime which also offers a significant source of income for many terrorist organizations. It has also recently gained great momentum. Various types of crime such as sexual exploitation, slavery (condition in which one human being was owned by another), forced employment (Use of men and young people as workers in job sites such as agriculture, livestock farms and construction), organ trafficking and kidnapping for ransom all come under the umbrella of this crime. In this article, the issue of inadequate international cooperation in the struggle against the financing of terrorism regarding human trafficking is discussed. In this study, the crime of human trafficking and the income obtained from this crime are handled in the context of terrorist organizations. Inadequate international cooperation is identified as the most significant challenge in the fight against the financing of terrorism. The three reasons that prevented international cooperation determined as a result of the literature research and they were listed as Inadequate Intelligence Sharing, Inadequate Legal Assistance Between Countries and Poor Border Controls Between Countries. The conclusion of this article, focuses on the importance of increasing international support, guidance, pressure and sanctions against the countries that offer inadequate cooperation to solve these problems preventing cooperation.*

Keywords: *Human Trafficking, The Relation between Human Trafficking and Terror, Financing of Terrorism, Financial Action Task Force, Insufficient International Cooperation*

[1] Captain, Phd Student at Marmara University, bilgin.birlikseven@hotmail.com

Introduction

Terrorism has various sources of finance such as the financial support of a state, income obtained from some legitimate enterprises, migrant smuggling, human trafficking (especially of women and girls), income obtained from illicit activities such as the sale of drugs and firearms, abuse of charitable donations, exploitation of the Hawala[2] system, theft, smuggling and malpractices especially concerning oil.[3] The income obtained from human trafficking is not the only source of funding for terrorist organizations but it can be observed that human trafficking has gained momentum recently[4] and that this crime attracts attention for both the link to terrorism and the human dimension.

Human trafficking is an important crime and a serious violation of human rights. Human trafficking is defined as an organized type of crime and this crime can be committed by a wide range of organizations, ranging from small gangs to large criminal and terrorist organizations. Every year, thousands of people, foremost being women and children, are entrapped and enslaved by traffickers. Almost every country in the world is either a source country, or transit country or a country of destination: and many people are affected by this crime.[5] There are also proven links between the income obtained from human trafficking and the financing of terrorism.[6] Moreover, the contribution of human trafficking to terrorist organizations is not only economic. Forced domestic service or employment in industry, the use of kidnapped or debited children in armed conflicts and sexual slavery, are all modern forms of slavery. It may be asserted that it is difficult to fully assess the true extent of the international organizational structure of human trafficking.[7]

The terrorist's need for funding of terrorism was clearly evidenced in a 2007 statement by Sheikh Mustafa Abu al-Yazid, the former leader of the al-Qaeda terrorist organization. In this statement, he stated that:

"*In Afghanistan, financing is one of the main needs of jihad. Taliban has thousands of combatants, but they need financing. There are hundreds of people who want to operate in order to reach the level of martyrdom, but they cannot find the funds to equip them. Therefore, financing is the backbone of jihad.*".[8]

The sheer volume of income derived from human trafficking worldwide and particularly in vulnerable regions such as the Middle East and North Africa, combined with the routine use of practices that show complete disregard for human dignity has attracted the attention of the world. Especially horrific is the manner in which women and children are commodified and their right to live in dignity taken away from them: this aspect appears prominently in most of the literature on the subject.

---

2 Money transfers conducted outside the informal banking system and through an unregistered, trust-based financial service network. (https://www.nato.int/docu/review/2007/issue2/turkish/analysis2.html).

3 NATO, "Money at the Root of Evil: The Economy of Transnational Terrorism ", (https://www.nato.int/docu/review/2007/issue2/turkish/analysis2.html), Accessed: 22 March 2019.

4 United Nations, "Identifying and Exploring The Nexus Between Human Trafficking, Terrorism, and Terrorism Financing", (https://www.un.org/sc/ctc/wp-content/uploads/2019/02/ht-terrorism-nexus-cted-report.pdf), s. 11, Access: April 26, 2019.

5 United Nations Office on Drugs and Crime, Traff Human Trafficking ", (https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html), Accessed: May 10, 2019.

6 Report, "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants July 2011",(https://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf), s. 39, Accessed: April 17 2019.

7 Hakan Erdal, "Human Trafficking as an Organized Crime Type and the Case of Turkey", *Journal of Police Sciences*, 10, 2, (2008), p. 79.

8 NATO, "Money at the Root of Evil: The Economics of Supranational Terrorism ".

Many challenges exist in the struggle against the financing of terrorism regarding human trafficking and these are detailed in various reports by international institutions and organizations: it may be asserted that the most important of these is a lack of international cooperation. For this reason, and for a lack of adequate attention to this aspect in the current literature, inadequate international cooperation in the struggle with the financing of terrorism regarding human trafficking was chosen as the focus of this study. This paper aims to contribute to filling the gap in the current literature.

In this article the issue is not treated within the context of any particular terrorist organization. Instead the focus is on the relationships of terrorist organizations with human trafficking. The focus of this article will be the existing initiatives to increase international cooperation (such as coercive sanctions), the factors preventing cooperation and alternative measures to increase international cooperation.

Five factors preventing international cooperation were determined during the literature review and these were then were reduced to three on the basis of some degree of the commonalities between them: *Inadequate Intelligence Sharing*, *Inadequate Legal Assistance between Countries* and *Poor Border Controls Between Countries*. The article emphasizes the importance of international cooperation in combatting human trafficking as an international crime. In fighting any kind of international criminal activity, international cooperation will be vital. This can be achieved under the guidance of international organizations such as the United Nations (UN) and Financial Action Task Force (FATF): sometimes by providing technical and financial support to the countries where the specific problems exist, sometimes by highlighting the human side of the problem and applying international pressure, sometimes by sanctions and in some cases by implementing a combination of these approaches, it may be ensured that the countries identified as exhibiting weaknesses may participate fully in an international coalition against the crime of financing terrorism through human trafficking. An analogy of this approach working in practice may by the cooperation in achieving the Iran Nuclear Deal, lead notably by the US, the EU and the Iranians themselves: international cooperation to bring a into the can be achieved.

This article is based on the most up to date reports mostly published by international institutions such as UN, FATF, Organization for Security and Cooperation in Europe (OSCE) and others. The article is structured as follows: in the first part, the conceptual framework of human trafficking is examined in relation to its interface terrorist organizations; in the second part, the numerical data of human trafficking will be explored; and in the final section, the article defines the problem of inadequate international cooperation in preventing the financing of terrorism and presents possible solutions.

Human Trafficking: Conceptual Framework

I. Definition of Human Trafficking

Although the crime of human trafficking is covered regularly by the news media and in social media, there is a general misconception about what exactly human trafficking is. The most prominent element of this misconception is mistaking human trafficking for migrant smuggling. Although the differences between human trafficking and migrant smuggling are not the subject of this article, it should be noted that the two types of crime are different from each other.

The most widely accepted definition regarding the crime of human trafficking was made by the UN in 2003. According to the Protocol on the Prevention, Suppression and Punishment of

Human Trafficking especially with Women and Children, which complements the United Nations Agreement against International Organized Crimes that entered into force on 25 December 2003 and is generally accepted as being the first international agreement regarding human trafficking.[9] Human Trafficking means the recruiting, moving, transferring, hosting or taking of people to exploit them by way of threatening or use of force or by other means such as force, abduction, fraud, deception, abuse of power or by taking advantage of a state of defenselessness or paying or helping someone who has control over a person to receive his/her approval.[10] From this definition we can say that any kind of use and exploitation of human without his/her consent as if s/he were a commodity, is relevant in human trafficking.

According to this protocol, exploitation includes the exploitation or forced labor of others through prostitution or other ways of sexual exploitation, service, slavery or similar implementations or the harvesting and selling of organs. In case of the victims of human trafficking, consent to exploitation is irrelevant with regard to this protocol: the exploitation must involve force. Again, within the context of the protocol, in case a child is employed, moved, transferred, harbored or taken for exploitation, even if it does not include any of the specific methods mentioned above, it is nonetheless accepted as human trafficking. A child is defined as anybody under the age of eighteen.[11] But even though not applicable for children, consensual state is a crucial detail in defining human trafficking as opposed to migrant trafficking, where the subjects are to a degree volunteers.

The protocol is aimed at preventing human trafficking, particularly of women and children, as well as ensuring the full respect and protection being given to the human rights of human trafficking victims as individuals.[12] Human trafficking is one of the most serious crimes an individual can commit against his/her fellow human beings. That those who are subject to this crime are predominantly women and children, who are often defenseless and in a more vulnerable state to a greater degree than adult men is understandable. Therefore, both human rights and the rights of women and children are attached particular importance in the protocol.

Although many measures have been taken by governments and non-governmental organizations related to human trafficking, the number of victims continues to increase. For example, according to the research of a private company named Statista, while the number of victims of human trafficking in the world in 2008 was 30,961, in 2017, this number was 100,409.[13] According to the report of the United Nations Office on Drugs and Crime (UN ODC) published in 2018 on human trafficking, the number of the victims of this crime peaked in 2016, by reaching a figure of more than 24,000, when the the previous 13-year period is considered. The United Nations Office on Drugs and Crime has collected data on approximately 225,000 human trafficking victims since the entry into force of the United Nations Human Trafficking Protocol in 2003.[14] It should be noted that these figures are the

9 FATF Report, "Money Laundering Risks Arising from Trafficking in Human Beings…", p. 11.

10 United Nations, "Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Suplementing the United Nations Convention Against Transnational Organized Crime", (https://treaties.un.org/doc/treaties/2000/11/20001115%2011-38%20am/ch_xviii_12_ap.pdf), p. 2, Access: April 19, 2019.

11 United Nations, "Protocol to Prevent, Suppress and Punish Trafficking in Persons", p. 2.

12 ibid, p. 2.

13 Statista, "Human trafficking - statistics and facts", (https://www.statista.com/topics/4238/human-trafficking/), Access: May 10, 2019.

14 United Nations Office on Drugs and Crime, "Global Report on Trafficking in Persons 2018", (https://www.unodc.org/documents/data-and-analysis/glotip/2018/glotip_2018_book_web_small.pdf), p. 21, Access: May 14, 2019.

numbers noted in the reports but the real numbers may be considerably more than that. These figures reveal the fact that human trafficking has gained momentum and that this crime does not seem easy to intercept in the medium term.

II. The Scope of the Crime of Human Trafficking

Both migrant smugglers and human traffickers become involved in these crimes to make a profit. While this profit is essentially financial in migrant smuggling, there are other, additional forms of profit available in human trafficking. According to human traffickers, human is a commodity. People can be bought and sold and exploited for various purposes.[15] As a result, terrorist organizations and human trafficking should not only be considered to be conducting the activity for financial gain. Terrorist organizations like ISIS may use the people they have commoditized for any purpose, seeing no issue with cognitively, and moreover considering the decision to be a practical necessity.

Terrorist organizations exploit the victims of human trafficking in various ways. The sale of the victims of human trafficking seems to be the most profitable method. The militants of ISIS may use their slaves as if they were their employees, exploit women and girls sexually and may force child slaves to cook, clean, wash and otherwise take care of them. Men, young people and children were used by ISIS as workers. This, of course, happened by force and the victims were often, in their period of servitude, also indoctrinated. The victims were forced to work in work areas such as agriculture, sheep and goat breeding, poultry farming and construction. Others were forced to build tunnels under the streets of Mosul: these tunnels were pivotal to the defence of the city.[16] Human trafficking can be seen to have clear benefits for the for the terrorist, both materially and in terms of boosting morale.

The flow of human trafficking is closely associated with armed conflict and may also involve sexual exploitation, forced labor and migrant smuggling in the area affected by the conflict.[17] According to a report by the United Nations, ISIS both sold trafficked Yezidi women back to their families for a ransom and also smuggled these women to Turkey and sold them to human traffickers and prostitution gangs.[18] ISIS militants found that they could make use of their slaves again and again as a re-usable commodity. An example of this is a 13 year old Yezidi who was detained for 11 months and sold several times. Unlike disposables (such as oil or antiquities), victims of human trafficking can be exploited many times and for various purposes.[19] The scope of the crime evolves until the commoditized human has lost its 'value'.

Organ trafficking, on the other hand, also appears in the context of financing ISIS. The source of these claims are the statements of ex-prisoners and former militants who have left ISIS. In an ISIS document alleged to be published by the Research and Fatwa Office of ISIS it is stated that "The lives and organs of those who have apostatized need not be respected and these lives and their organs can be taken from them without any penal sanctioning," meaning the collection of the organs of non-Muslims is permissable in this case. While all of these do not necessarily provide concrete evidence

---

15 United Nations, "Identifying and Exploring The Nexus Between Human Trafficking,....", p. 12.

16 United Nations, "Identifying and Exploring The Nexus Between Human Trafficking,....", p. 33.

17 FATF Report, "Financial Flows from Human Trafficking July 2018", (https://www.fatf-gafi.org/media/fatf/content/images/human-trafficking-2018.pdf), p. 12, Access: 26 April 2019.

18 United Nations, "Identifying and Exploring The Nexus Between Human Trafficking,....", p. 34.

19 ibid, p. 32.

that ISIS is organ trafficking, the possibility of ISIS' making money from organ trafficking is very real.[20] As a result, this element of human trafficking should also be considered.

Criminal organizations dealing with human trafficking are increasingly interacting with local contacts to provide transport, safe houses and fake documentation. Human traffickers are also often involved in crimes such as drug trafficking in coordination with their other criminal activities. Victims of human trafficking are often used as drug couriers or are forced to commit other crimes such as petty theft.[21] In the information presented at the Cape Town workshop by the Intergovernmental Action Group against West African Money Laundering, it was also stated that there is a strong link between human trafficking and various other crimes and corrupt activities in West Africa.[22]

Victims are trafficked by being kidnapped or deceived.[23] There is evidence that criminal networks involved in human trafficking routinely target the most vulnerable people, especially women and children.[24] A number of false promises are made by terrorist or transnational crime organizations, exploiting the victims' dreams of security and economic opportunity which subsequently turn into the nightmares of slavery and forced prostitution. In the literature on human trafficking it is often noted that women and girls are priority targets and are routinely subjected to sexual exploitation. Therefore, it can be stated that society's most sensitive group in terms of human trafficking is women and girls. This sensitive mass can provides both a material resource and a source of morale for the terrorist organisations.

III. Nexus Between Human Trafficking and Terrorist Organizations

There is identifiable link between terrorist organizations and human trafficking because terrorist organizations create the conditions for the trade through the conflicts they have caused. Terror campaigns cause the displacement of people, rendering those people vulnerable. Displaced people become susceptible to migrant smuggling networks or are exposed to the abuse and exploitation of human trafficking networks through similar channels.[25] In areas where government authority breaks down and dominance lies in the hands of terrorist organizations, laws are rewritten by the terrorists with their own interpretations: many previously illegal activities may become 'legal'. Human trafficking is often one of them.

It is known that terrorist organizations such as the PKK, ISIS, Somalia's al-Shabaab, the Syrian al-Nusra Front, al-Qaeda in the Arabian Peninsula, Nigeria's Boko Haram and the Abu Sayyaf Group all generate income from human trafficking. The PKK terrorist organization, which is one of the most important terror problems for Turkey, has generated a considerable income from human trafficking.[26] In a report published by Europol in 2011 it is clearly stated that the PKK generates

[20] ibid, p. 36-37.

[21] FATF Report, "Money Laundering Risks Arising from Trafficking in Human Beings…", p. 12.

[22] ibid, p. 39.

[23] United Nations, "Report on the Secretary-General on Conflict Related Sexual Violence", (https://www.un.org/sexualviolenceinconflict/wp-content/uploads/report/s-2018-250/SG-REPORT-2017- CRSV-SPREAD.pdf), p. 7, Access: April 22, 2019.

[24] FATF Report, "Financial Flows from Human Trafficking July 2018", p. 12.

[25] FATF Report, "Financial Flows from Human Trafficking July 2018", p. 16.

[26] Police Academy Publications, "Terror Threat to Humanity and Democracy: the Case of PKK", (https://www.pa.edu.tr/Upload/editor/files/PKK_Ornegi_Raporu_TR.pdf), p. 27, Access: April 12, 2019.

revenue from human trafficking.[27] In a statement made by the Republic of Turkey's Ministry of Interior in January 2019, it was also stated that the PKK is an organization that participatesin both human and drug trafficking.[28] Human trafficking is an important element in the financing of terrorism.

The displacement of indigenous people in many conflicted parts of the world, thus increasing vulnerability of those people, human trafficking has been gaining popularity with terrorist organizations and other criminal organizations that seek out such opportunities.[29] Terrorist organizations have made good use of the so-called Arab Spring in the Middle East to generate funding from human trafficking. As a result, there has seen a significant increase in human trafficking across the Middle East.[30] In recent years, the number of victims of human trafficking has increased, together with irregular migration and the number of displaced persons. The direction of trafficking is mostly outwards from the conflict zone. The requirements of terrorist organizations creates a push factor for terrorist organizations' attempts to obtain finance from human trafficking in the Middle East. As a pull factor, terrorist's individual preference and pragmatist point of view (i.e. sexual exploitation) can be said.[31]

IV. Push and Pull Factors for Human Trafficking[32] [33] [34]

Number	Push and Pull Factors for Human Trafficking	
	Push Factors	**Pull Factors**
1	The interests and demands of terrorist organizations	Individual preference and pragmatist perspective
2	The use of human trafficking victims as a courier in drug trafficking, which is a major gain	Displacement of indigenous people in conflict zones in the world and thus, together with the increase in defenselessness and vulnerability, terrorist organizations taking this opportunity to head towards human trafficking
3	The desire to put pressure on local people in conflict zones and ideological reasons	To earn income
4	That local people who want to escape from conflict zones become victims of human trafficking for various reasons as they contact criminals and terrorist organizations, wanting to become immigrants	Sexual exploitation

27 EUROPOL, "EU Terrorism Situation and Trend Report 2011 Report", Report, (2011), p. 22.

28 Republic of Turkey Ministry of Interior, "The PKK is an Organization of Human Trafficking and Drug Trafficking" (https://www.icisleri.gov.tr/pkk-bir-insan-kacakciligi-ve-uyusturucu-ticareti-orgut), Access: May 18, 2019.

29 ibid., p. 74.

30 Yasemin Ozdek, "Kuresel Yoksulluk ve Kuresel Siddet Kıskacında Insan Hakları", p. 29.

31 FATF Report, "Financial Flows from Human Trafficking July 2018", p. 12-16-74.

32 Ibid, p. 16.

33 United Nations, "Identifying and Exploring The Nexus Between Human Trafficking,…", p. 30.

34 The United Nations Office on Drugs and Crime, "What are the root causes of trafficking?", (https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_9-2.pdf), pp. 454-455, Access: October, 19, 2019.

5	That some parents sell their children for a better life and a future rather than money	Use of child slaves for cooking, cleaning, washing and taking care of terrorists
6	That the insignificance of women and girls in some societies render them vulnerable to trafficking	Use of men and young people as workers in job sites such as agriculture, livestock farms and construction (such as employing victims of trafficking in tunnels built under the streets of Mosul)

V. The Nexus Between Organized Crime Organizations and Terrorist Organizations

With the increase of the number of unstable and economically challenged countries in the post-Cold War period and important developments in communication technologies, the nexus between terrorists and organized crime organizations has also changed and developed. This new dimension of the relationship has attracted more attention since the September 11 attacks. While the main objective of organized crime organizations is to earn money easily through illegal activities, the aim of terrorist organizations is to secure the financing they need to achieve their ideological goals. The common purpose of earning income combined these two illegal organizations and enables them to cooperate. From time to time, this connection is established with cooperation in areas such as training (military training and using offshore bank accounts), intelligence sharing, and mutual protection activities.[35] For example, hybrid structures formed by organized crime organizations and terrorists in Libya have combined to engage in human trafficking there.[36] Of course, there is not always a relationship between these two illegal organizations: while terrorists and organized crime organizations work together from time to time, they may sometimes experience a conflict of interest or even be in direct competition.[37]

Human Trafficking as the Financial Source of Terrorism

I. The Relationship between Financing Terrorism and Human Trafficking

According to a report published by the UN, human trafficking not only plays a key role in the context of terrorist organizations' strategy of subjugation, control and imposing their ideology on vulnerable communities, but also as a lucrative source of income.[38] A report issued by the United Nations Secretariat on 29 March 2019 emphasized the nexus between sexual violence, human trafficking and the financing of terrorism.[39]

---

35 İsmail Sarı, "The Nexus Between Terrorism and Organized Crime; Growing Threat?", (https://dergipark.org.tr/tr/download/article-file/155620), p. 464-477, Access: October, 22, 2019.

36 United Nations, "The nexus between human trafficking and terrorism",(https://www.un.org/sc/ctc/wp-content/uploads/2018/11/2.-Ms-Delphine-Schantz-CTED.pdf), Access: October, 20, 2019.

37 Mullins, Sam, and James K. Wither. "Terrorism and Organized Crime." *Connections*, vol. 15, no. 3, 2016, pp. 65–82. *JSTOR*, www.jstor.org/stable/26326452. p. 71.

38 United Nations, "Identifying and Exploring the Nexus Between Human Trafficking,....", p. 30.

39 United Nations, "Conflict Related Sexual Violence, Report of the united nations secretary-general",(https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/04/report/s-2019-280/Annual-report-2018.pdf), p. 6, Access: October, 21, 2019.

The FATF report issued in June 2018 shows the nexus between human trafficking and the financing of terrorism. For example, it is noted that terrorist organizations such as ISIS, Boko Haram and al-Shabaab use human trafficking to fund their organizations and their activities.[40] ISIS actively encourages its militants by praising human trafficking, especially that of women and children in *Al Dabiq*, its own media organ. Moreover, there is even ISIS guidance on how many female slaves militants can keep.[41] It is also estimated that there is a link between the financing of terrorist organizations (i.e. Provisional Irish Republican Army[42]) and human trafficking in Ireland.[43] The crime of human trafficking is not only a source of income but also a source of personnel for terrorist organizations.[44]

In the decisions 2331 (2016) and 2388 (2017) issued by the UN Security Council, it is emphasized that, among other purposes of human trafficking, it is used as a means of increasing the financing of terrorism.[45] The report issued by the United Nations also contains information on this. For example, that on March 27, 2017, the Kenyan police arrested an ISIS terrorist named Ali Hüseyin Ali, who is described as a key link not only in migrant smuggling and human trafficking but also in the financing of terrorism. This is embodiment of the use of human trafficking in the financing of terrorism.[46] Likewise, the systematic sale of Yezidi women by ISIS can be regarded as one of the most prominent examples of generating income for the terrorist activities.[47]

Terrorist organizations can also benefit from the ransom received from families. Families use different ways to send money to the terrorist groups so that these terrorist groups can conceal to the ransom payments, especially which come from different countries.[48] It may not be possible to determine the revenues obtained in this way at all times.

II. Economic Aspect of Human Trafficking

According to the report published by the FATF in 2018, originally founded in Paris in 1989 by the G-7 Summit in response to concerns about money laundering[49], human trafficking stands out as one of the most profitable criminal activities in the world. It is estimated that generating an annual income of $150.2 billion.[50]

According to Europol, human trafficking is one of the most lucrative types of organized crime. It has a wide range of interest groups, ranging from small criminal organizations to terrorist organizations. For example, while human trafficking in Europe is controlled by Russian and

40 FATF Report, "Financial Flows from Human Trafficking July 2018", p. 38.

41 FATF Report, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", (http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist- organization-ISIL.pdf), p.13, Access: April 22, 2019.

42 Independent, "PIRA figures are 'involved in human trafficking operation'" (https://www.independent.ie/irish-news/pira-figures-are-involved-in-human-trafficking-operation-31481500.html), Access: January 6, 2020.

43 FATF Report, "Money Laundering Risks Arising from Trafficking in Human Beings…", p. 40.

44 Selahattin Gürel, "Financial Resources of Terror and Terrorist Organizations", *International Journal of Management and Social Research*, 2, 4, (2015), p. 20.

45 United Nations, "Identifying and Exploring the Nexus Between Human Trafficking,....", p. 30.

46 Ibid, p. 13.

47 ibid, p. 30.

48 FATF Report, "Financial Flows from Human Trafficking July 2018", p. 16.

49 The Financial Action Task Force, "History of the FATF", (http://www.fatf-gafi.org/about/historyofthefatf/), Access: May 13, 2019.

50 FATF Report, "Financial Flows from Human Trafficking July 2018", p. 74.

Albanian gangs and Italian mafia, in Asia, they are controlled by Chinese criminal organizations and the Japanese Yakuza.[51]

Women seized by terrorist organizations are exhibited in slave markets in the areas where they are held. Those interested in these women can check their hair, teeth, or ask them to walk in order to better observe them if they like. The sum demanded by the terrorist organization from the prospective buyer for these women may vary depending on the women's marital status, age, number of children and their beauty as evaluated by the buyer on their own terms. Estimated price range is between $1,500-200. Other criteria are also considered for pricing. For example, $172 was the established for those between 0-9 years, $129 for those between 10-20 years, $86 for those between 20-30 years and $75 for those between 30-40 years. In some cases, slaves were offered free of charge.[52]

Kidnapping for ransom appears to be one of the key elements of the finance strategies of terrorist organizations. Kidnapping for ransom engenders insecurity and also provides a very high financial gain if successfuln. With the awareness of the threat of kidnapping for ransom, the UN Security Council often calls on member states to prevent terrorists from benefiting directly or indirectly from ransom payments or political privileges granted to ensure the safe release of hostages. It is known that many terrorist organizations, notably ISIS, al-Nusra Front, al-Qaeda in the Arabian Peninsula, Boko Haram and Abu Sayyaf Group, all continue to generate income from kidnapping for ransom. Families are required to pay between $10,000-40,000 to ensure the release of family members held hostage by. It is estimated that $850,000 was paid to ISIS for the release of 200 Iraqi Yezidis in January 2015.[53] For ISIS, which is notorious for its kidnapping activities, ransom payments are an important source of income as of 2014. It is estimated that in 2013, ISIS generated around $96,000-123,000 a day from ransom.[54] According to the United Nations Iraqi Aid Mission, ISIS generated between $35-45 million from ransom payments made by hostages' families in 2014.[55] While financial resources such as natural resources and taxation are more profitable for terrorist organizations, human trafficking is also an important source of income for terrorist organizations.[56]

Inadequate International Cooperation

I. Initiatives to Increase International Cooperation

A. Financial Action Task Force

Despite ISIS' loss of territory, many states around the world continue to face the threat of some form of terrorism or terrorist financing since 2016.[57] This situation is not solely limited to ISIS.

51 FATF Report, "Money Laundering Risks Arising from Trafficking in Human Beings…", p. 12.

52 United Nations, "Identifying and Exploring the Nexus Between Human Trafficking,....", p. 31.

53 United Nations, "Identifying and Exploring the Nexus Between Human Trafficking,....", p. 35.

54 United Nations, "Security Council S/2014/815 ", (https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_815.pdf), Access: April 22 2019.

55 United Nations, "Council Security Council S/2014/770", (https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_770.pdf), Access: 24 April 2019.

56 United Nations, "Identifying and Exploring The Nexus Between Human Trafficking, Terrorism, and Terrorism Financing", (https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf), p. 9-31, Access: October 22, 2019.

57 The Financial Action Task Force, "2017-2018 Annual Report", (http://www.fatf-gafi.org/media/fatf/documents/brochure-sannualreports/FATF-annual-report-2017-2018.pdf), p. 12, Access: May 26, 2019.

Different terrorist organizations in various locations continue to exist as the source of this threat. Therefore, the struggle with the financing of terrorism that concerns all countries stands out as a total international struggle, which cannot be carried out with the individual struggles of the states. In this sense, the FATF has an important mission in this global struggle.

FATF was established in Paris in 1989 by G-7 members as a response to growing concerns about money laundering.[58] This international organization has a total of 38 members, 36 of which are state and 2 are regional organizations.[59] FATF's recommendations on the struggle with money laundering and the financing of terrorism and its coordinated studies with the member states play an important role in the struggle with human trafficking as a source of finance for terrorist organizations. The objectives of the organization are to set standards and promote the effective implementation of legal, regulatory and operational measures for the integrity of the international financial system in the struggle with money laundering, financing of terrorism and other relevant threats.[60]

It may be asserted that FATF,[61] which Turkey is also a member of has strict control over the member states. Therefore, the member states choose to fill the deficiencies related to the recommendations of the organization immediately. The reason for this is the effective sanction power of FATF on the member states. With the resolutions made at the General Assembly of FATF, some countries can be considered risky by the assertion of their deficiencies regarding the financing of terrorism and their commercial relations may be damaged. These sanction decisions can be listed as follows:[62] removing the countries, which do not meet organizational standards from membership; forcing the relevant country financial institutions[63] to implement the strict "know your customer" measures; initiating a systematic or strict reporting mechanism regarding the financial transactions of the country concerned; not to allow international financial institutions to open branches or representative offices in the sanctioned country; restriction of commercial or financial transactions with the sanctioned country or persons in that country; obliging international financial institutions to review, change or, when necessary terminate their connections and relations with financial institutions in the sanctioned country; to require increased audit reviews for branches and affiliates of financial institutions in the sanctioned country. With such sanction mechanisms, members are almost forced into international cooperation.

The annual meetings of the Organization are attended by experts from FATF Style Regional Bodies in different parts of the world and from international organizations such as IMF, UN and World Bank. This makes a great contribution to the exchange of ideas on current and emerging money laundering and terrorist financing risks and raising overall awareness.[64] In addition to these regular meetings, the organization also publishes reports on the financing of terrorism. FATF has

58 The Financial Action Task Force, "History of the FATF".

59 The Financial Action Task Force, "FATF Members and Observers", (http://www.fatf-gafi.org/about/membersandobservers/#d.en.3147), Access: May 11, 2019.

60 The Financial Action Task Force, "Who we are", (http://www.fatf-gafi.org/about/), Access: May 13, 2019.

61 The Financial Action Task Force, "Countries FATF membersHttps, (https://www.fatf-gafi.org/countries/#FATF), Access: May 10, 2019.

62 Ministry of Justice General Directorate of Foreign Relations and European Union, "FINANCIAL ACTION DUTY STRENGTH, SANCTION MECHANISM", (http://www.uhdigm.adalet.gov.tr/fatf/yaptirim_mekanizmasi.html), Access: April 29, 2019.

63 For more information, see: (https://www.tbb.org.tr/dosyalar/arastirma_ve_raporlar/bankacilikta_operasyonel_risk.pdf).

64 The Financial Action Task Force, "FATF / MONEYVAL Joint Experts' meeting 25-26 March 2019", (http://www.fatf-gafi.org/publications/methodsandtrends/documents/jem-2019.html), Access: 12 May 2019.

a developed institutional structure and constantly works hand in glove with its members. In the context of international cooperation in the struggle against the financing of terrorism, it can be said that international cooperation is theoretically at a good level, judging by the number of meetings, forums and workshops.

Since the events of 9/11, FATF has played a leading role in global action in the struggle with the financing of terrorism. It has been developing global standards in the struggle with the financing of terrorism, and to which more than 200 jurisdictions are committed. As a result, all states now consider the financing of terrorism a crime and are taking concrete steps to detect, disrupt and deter it. But more needs to be done. FATF assesses the progress of countries and helps its members to take action.[65] In various FATF reports, it is emphasized that the fight against terrorist financing is the main priority and it is also stated that terrorism continues to affect security, democracy, freedom and the desire to live in mutual understanding, peace and tolerance. However, the organization emphasizes the need to focus on regional strategic planning and close cooperation with the Global Network of FATF and FATF Style Regional Bodies, taking into account the regional nature of some threats. As of 2019, FATF continues its activities under the presidency of the USA. Again in this period, fighting against the financing of terrorism continues to be the primary target.[66] Within the context of the issues mentioned above, it is seen that there is a great effort and work towards international cooperation in discursive and written form.

B. Emphasis on International Cooperation in Some FATF Meetings and Reports

In this section, a total of four international meetings from 2017, 2018 and 2019 are presented as examples to illustrate the current situation. Only international meetings in 2017, 2018 and 2019 are handled here, as the both meetings held in these years provide a summary of the general situation and the current situation is wanted to be presented.

1. FATF UN Meeting (2017)

Santiago Otamendi, president of the organization in the 2017-2018 term, highlighted another important aspect of the financial activities and channels of terrorists in his speech at the UN Anti-Terrorist Committee Briefing in December 2017. According to Otamendi, regardless of the size and complexity of these financial activities, it is important that they are a source of intelligence. because, thanks to this information, it will be possible to identify terrorist cells, the people they are connected with, those who aid and abet them and the structural models of these groups.[67] Thus, there is also a reference to international cooperation here.

2. Argentina (2018)

In 2018, under the presidency of Argentina, a new Operational Plan to Combat Terrorist Financing was agreed upon. This new plan provided a renewed focus for the studies of FATF. In this plan, it was aimed to help address the security gaps in countries' regimes devoted to struggling with the

[65] The Financial Action Task Force, "International conference on combating the financing of Daesh and Al-Qaeda",(http://www.fatf-gafi.org/publications/fatfgeneral/documents/no-money-terror-apr-2018). html), Access: May 11, 2019.

[66] The Financial Action Task Force, "2017-2018 Annual Report ", p. 13.

[67] Ibid, p. 11.

financing of terrorism and it included a series of projects and activities designed to understand and respond to newly emerging threats. It is seen that a consensus was built for this new plan to remain flexible and adaptable in order to address the security gaps of FATF, also observed during the 2019 US presidency period and to cope with the emerging threats.[68]

In 2016, in line with the Unified Strategy for Struggling with Terrorist Financing, which was recognized as a response to the strengthening of the nature and scope of worldwide terrorist threats, including ISIS, the Operational Plan focuses on improving and updating the understanding of terrorist financing risks, promoting more effective coordination including the sharing of information at home and abroad, ensuring that FATF standards provide up-to-date and effective tools in struggling with terrorist financing and also ensuring that the tools are effectively applied including targeted financial sanctions.

3. France (2018)

On April 26, 2018, FATF convened an international conference on the struggle against ISIS and the financing of Al-Qaeda at the invitation of French President Emmanuel Macron under the slogan "No Money for Terror". This conference not only raised awareness concerning this issue but also provides an opportunity to strengthen the joint response to the financing of terrorism.[69] After the meeting in France, the final declaration was welcomed by FATF, and a high level of commitment was given to participation in the judicial approaches, encouraging the collaboration of sub-organizations and the prevention of the monetary flow to areas affected by terrorism. It is seen that FATF is looking forward to further concrete steps, including the strengthening of cooperation with public-private partnership and more importantly, continuous political will and capacity to act.[70]

With this meeting, the importance of a holistic approach to the struggle with terrorism and the financing of terrorism was emphasized. The aim was to increase overall national and collective participation based on the commitment to the struggle with all terrorist organizations and their financing in the struggle with the initiatives and assets regarding the ISIS and Al-Qaeda terrorist groups. The following decisions were made: further strengthening the legal and operational structure for the collection, sharing and analysis of data by national authorities, struggling with anonymous financial transactions, increasing the traceability and transparency of non-profit organizations and aid funds, anticipating and addressing the risk of the misuse of new financial instruments, cooperating with the private sector, especially with the technology in the struggle with the financing of terrorism, not to ignore the significant contribution of the freezing and seizure mechanism of international and national assets, to increase the effectiveness of international cooperation, to support the authority, visibility and opportunities of FATF and FATF Style Regional Bodies, strengthening joint responsibility against states that do not have sufficient standards or capacity and lastly, maintaining joint mobilization against terrorist financing.[71]

---

68 The Financial Action Task Force, "2017-2018 Annual Report ", p. 12.

69 The Financial Action Task Force, "International conference on combating the financing of Daesh and Al-Qaeda",(http://www.fatf-gafi.org/publications/fatfgeneral/documents/no-money-terror-apr-2018). html), Access: May 11, 2019.

70 ibid.

71 France Diplomatie, "Final statement - International conference on combating the financing of Daesh and Al-Qaeda (Paris, 25-26.04.18)", (https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/events/article/final-statement-international-conference-on-combating-the-financing-of-daesh), Access: May 10, 2019.

4. Israel (2019)

At the Joint Experts Meeting held by FATF in Tel Aviv, Israel, on 25-26 March 2019, the key role of the organization in identifying new and emerging risks regarding the financial system, including money laundering, terrorist financing or the proliferation of financing, was highlighted.[72] On 27 March 2019, again, a workshop was held in Tel Aviv to investigate the terrorist financing and increase the capacity of filing suits.[73] Attempts to increase cooperation were to be accelerated through this meeting and workshop, because cooperation between countries with regard to investigation and litigation is of great importance in this struggle.

C. EGMONT Group

The Egmont Group is a joint body, which consists of 158 Financial Intelligence Units worldwide. This organization offers reliable expertise and financial information exchange service to combat money laundering and terrorism financing. These Financial Intelligence Units are particularly important because they are positioned to support national and international cooperation against the financing of terrorism and are a reliable method for sharing financial information both domestically and internationally in accordance with the international standards of struggling with money laundering and the financing of terrorism. The Egmont Group constitutes the operational strength of FATF and provides the organizational structure against international money laundering and the financing of terrorism. The Egmont Group acknowledges that the sharing of financial intelligence is very important and is the cornerstone in the struggle against money laundering and terrorism financing in the international arena. Financial Intelligence Units around the world are obliged to exchange information and cooperate internationally in accordance with the standards of the struggle with international money laundering and terrorism financing. As an international financial intelligence forum, Egmont Group directs and facilitates the process that takes place among its members.[74]

The Financial Crimes Investigation Board, also known as MASAK in Turkey, is a member of the Egmont group. MASAK's mission is "*to contribute to the policy and regulation making for the prevention and detection of money laundering and terrorist financing offenses, to collect and analyze information quickly and reliably, to conduct research and analysis and to communicate the obtained information and results to the relevant authorities.*".[75]

Terrorist organizations and criminals use various mechanisms and techniques to conceal their incomes and their assets obtained through criminal activities. The identification of the real owners of such assets is a major obstacle for prosecutors, law enforcement operatives and intelligence agencies around the world. In this sense, the prevention of abuse of legal entities and certain regulations is a very important topic for the whole international community including G-20 and FATF. In 2018, FATF and the Egmont Group published a joint report on security vulnerabilities related to the privacy of profitable property.[76]

---

72 The Financial Action Task Force, "FATF / MONEYVAL Joint Experts' meeting 25-26 March 2019", (http://www.fatf-gafi.org/publications/methodsandtrends/documents/jem-2019.html), Access: May 12, 2019.

73 The Financial Action Task Force, "Improving the capacity to prosecute terrorist financing", (http://www.fatf-gafi.org/publications/methodsandtrends/documents/jem-judges-2019.html), Access: May 14, 2019.

74 Egmont Group, "About", (https://egmontgroup.org/en/content/about), Access: April 19, 2019.

75 Financial Crimes Investigation Board, "VISION & MISSION", (http://www.masak.gov.tr/tr/content/vizyon-misyon/38), Access: May 12, 2019.

76 The Financial Action Task Force, "2017-2018 Annual Report ", p. 28.

D. Emphasis on the Inadequate International Cooperation of Other International Organizations

In a report published by the Council of Europe's Parliamentary Assembly's Committee on Political Affairs and Democracy in 2018, states are encouraged to cooperate more and coordinate with each other and with international structures established to counter this threat in the struggle with the financing of terrorism with the income obtained from human trafficking and other crimes.[77] UN Resolution 2253 also proposes that member states should cooperate fully with each other, that information sharing practices between governments should be developed, and that requests regarding the individuals and organizations supporting the ISIS terrorist organization should be listed more quickly. In a report published by the OSCE in 2014, it was emphasized that international cooperation is not adequate: "The speed of international cooperation on criminal matters cannot reach the speed of cross-border movement of goods and people.".[78]

International cooperation between source, transit and destination countries is not sufficient in human trafficking. It could be argued that some of these countries have hindered the struggle against human trafficking. Many source countries do not respond adequately and in a timely manner to international requests for information\necessary for transit and destination countries. Despite the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children signed in Palermo in 2000, which many source countries were party to, many of the source countries concerned have not yet implemented legislation that facilitates and enhances international cooperation in the fight against human trafficking. Prosecutors often wait for a long time, even for years, to obtain financial information on human trafficking, witness statements and evidence from foreign jurisdictions. But speed is very important during financial investigations. This is because delays in the freezing, apprehension and seizure processes of human trafficking cause serious damages to the investigations and restrict the scope and effectiveness of these investigations. Non-co-operating countries with bank account confidentiality laws and those reluctant to question financial institutions in their own country pose serious challenges in the investigation of human trafficking. There may also be difficulties in the exchange of information between different types of Financial Intelligence Units in the context of cooperation. Although all financial intelligence units share general functions such as the acquisition, analysis and dissemination of Suspicious Transaction Reports and other evidences, the structure of financial intelligence units is still very diverse and the differences in the legal powers of financial intelligence units remain a challenge for both timing and the international exchange of data. At this point, the EGMONT Group, where different Financial Intelligence Units are gathered under one roof, can play an important role. Some countries also face internal procedural barriers to the freezing, takeover and seizure of income generated from human trafficking in another country.[79]

The favorable position of some countries in the context of human trafficking and weak control measures, particularly in the Middle East and North Africa region, (to the terrorist at least) are expanding the field of activity regarding many types of crimes and increasing profits obtained from

---

[77] Council of Europe, Parliamentary Assembly, Committee on Political Affairs and Democracy, "Funding of the terrorist group Daesh: lessons learned", (http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp ? fileid = 24506 & lang = en), Access: May 23, 2019.

[78] Organization for Security and Co-operation in Europe, "Leveraging Anti-Money Laundering Regimes to Combat Trafficking in Human Beings", (https://www.osce.org/secretariat/121125?download=true), p. 21, Access: October 17, 2019.

[79] Organization for Security and Co-operation in Europe, "Leveraging Anti-Money Laundering Regimes to Combat Trafficking…".

these crimes, including human and migrant smuggling. According to a report published by the United Nations Office on Drugs and Crime, international cooperation in many fields for preventing these crimes remains inadequate.Therefore, cooperation between the neighboring countries inevitably becomes necessary in all areas in order to prevent human trafficking and the income derived from it, especially border controls and legal legislation, because it can be seen that cross-border coordination and cooperation between the countries in this region and their sub-regions is weak.[80]

II. Factors that Hinder International Cooperation and Possible Solutions

In order to ensure international cooperation, many meetings are organized, decisions are taken and organizations such as FATF are forced to cooperate through the sanction power. In the meetings held and reports published, it is apparent that international cooperation is weak and needs to be improved. Examining these meetings and reports, it can be seen that there is a strong will for international cooperation, but this situation is not reflected in the field. Factors preventing international cooperation identified in the literature can be grouped under the following five headings by utilizing their similarities:

1. Delays in obtaining information at international level,
2. Missing answers given to the requested information,
3. Restrictive conditions regarding information sharing,
4. Poor functioning of mutual legal aid processes[81],
5. The instability and poor border controls of countries at the micro level and the regions at the macro level.[82]

The first three factors listed above are problems related to the flow of information between countries. Therefore, we can gather the first three items above under the title of ”Inadequate Intelligence Sharing”. In spite of all the rhetoric and decisions taken in the context of international cooperation, the question of whether some countries have any reservations about the sharing of this information springs to mind. Could these problems be based on technical reasons? Although it is not possible to give precise answers to these questions, in view of the fact that corruption is widespread in countries where there is instability and the institutions of the state are underdeveloped, the possibility of some public officials‘ controlling the money flows based here and not reporting them as suspicious transactions may be inferred. At the aforementioned Cape Town Workshop it was suggested that there is a strong link between human trafficking and corruption. In this case, two options present themselves. The first is the enhancing of institutionalization in such underdeveloped countries through organizations such as FATF and other countries, and the second is the implementation of the aforementioned sanctions by FATF and other countries, on countries where corruption is institutionalized and cannot be prevented.

---

80 The United Nations Office on Drugs and Crime, “Combating Illicit Trafficking, Organized Crime and Terrorism”, (https://www.unodc.org/middleeastandnorthafrica/en/regional-programme-framework/trafficking-crime-and-terrorism/trafficking-crime-and-terrorism.html), Access: October 19, 2019.

81 FATF Report, “Financial Flows from Human Trafficking July 2018”, p. 35.

82 United Nations Office on Drugs and Crime, “Combating Illicit Trafficking, Organized Crime and Terrorism”, (https://www.unodc.org/middleeastandnorthafrica/en/regional-programme-framework/trafficking-crime-and-terrorism/trafficking-crime-and-terrorism.html), Access: May 10, 2019.

It is also possible that, due to the internal laws of the countries, people cannot share private bank information and other technical problems arising from information or systemic deficiencies. In this case, the solution of the problem seems relatively easy. FATF and Egmont Group are, however, in communication with member countries. If there are technical problems regarding this information transfer, a roadmap for their solution can be drawn and these problems can be solved. Again, it may be possible to make the necessary legal arrangements with the support of institutions such as FATF and international cooperation in the solution of the existing problems in the context of legal legislation. What is important here is the sincerity that countries show with regard to this issue.

The problem of weak legal processes, is examined under the title of "Inadequate Legal Assistance Between Countries". Here, it is the legal technical aspect that comes to the fore. First of all, the ratification of international conventions on legal aid by all countries and, more importantly, their implementation is of vital importance in this struggle. However, the countries that have ratified the convention should have accepted the judicial assistance process, its scope and the articles it is composed of as far as possible and without reservation. If, for example, the locations of the crime and originalating state of the perpetrator are different, the functioning of an effective trial process will be hindered unless a reservation is made on the agreement. For this hurdle to be crossed, it may be provided that the countries falling behind in mutual assistance participate in the agreements concerned or that they do what these agreements, which they are parties to necessitate with the pressure of the international community, by the international institutions and organizations', foremost being UN, drawing attention to the harm done by terror and human trafficking to international community and human dignity.

Since all the details cannot be regulated in international conventions, the content of this framework must feature special agreements made between the countries where human trafficking is at its most dense, by accepting these agreements as a framework, regarding judicial assistance in countries where the crime of human trafficking is committed as prime and on condition that this framework is not digressed from. For instance, if the witnesses of a human trafficking crime committed in Iraq are abroad, the legal aid institutions have to operate in a way that avoids wasting time in the process of securing statements in order to ensure an effective and fair trial.

The last factor, instability, is a prominent problem within the context of international cooperation, especially in the Middle East and North Africa. The Middle East and North Africa are particularly vulnerable to this crime: permanent instability in these regions provides an rich environment for human trafficking. This problem is examined under "Poor Border Controls Between Countries". Due to the strategic position of the Middle East and North Africa, chronic instability in some countries and relatively weak control measures in others, drug trafficking and associated illegal activities, such as the smuggling of firearms and migrants and human trafficking itself are all expanding. The increase in earnings from these activities are being transmitted to international and local criminal organizations alike.

Initiatives to prevent further development of organized crime, trafficking and drug trafficking require countries to develop strong and effective control of their borders. In this context, the objectives of preventing illegal smuggling activities and dissolving criminal organizations gain a particular importance. The biggest obstacle is the weak cross-border cooperation. It could be argued that the instability of regions at the macro level and the countries at the micro level facilitates the

financing of terrorism based on human trafficking in the absence of cooperation between countries. This problem seems to be the most difficult to solve. Especially because of the rich oil and natural gas resources, this region is constantly witnessing the struggle of various power centers. It would be a very optimistic expectation that international organizations, especially the UN, will ensure stability in the region in the near or medium term. Even if this cannot be achieved, given the urgency of the problem, countries in the region could/should take steps to prevent the crime of human trafficking. Providing technical, logistical and financial support to such countries within the scope of these joint studies will encourage them to take measures related to border controls.

Conclusion

In general in order to achieve this, the humanitarian dimension of the issue should be emphasized and joint studies conducted under the leadership of the UN to increase border controls in the countries with the heaviest traffic. The international dimension of the problem of financing terrorism in relation to human trafficking necessarily carries the struggle with this crime to the international dimension, and thus international cooperation inevitably becomes imperative. However, although there are many problem areas in the struggle with the financing of terrorism in relation to human trafficking, inadequate international cooperation seems to be the most important one. Although international cooperation in the fight against this crime has been brought forward regarding the relevant international organizations and some sanctions have been imposed and measures have been taken for this purpose, some of the obstacles to this cooperation have been mentioned above.

These five factors which prevent international cooperation can be discussed under three different headings. These may listed as Inadequate Intelligence Sharing, Inadequate Legal Assistance between Countries and Poor Border Controls between Countries. If we should summarize the solution proposals under these headings:

Inadequate Intelligence Sharing: There may be two reasons for insufficient flow of information between countries, the first being deliberately not sharing information and the other technical reasons. According to a general assumption, corruption is more common in countries with less institutionalization. From this point of view, it is possible to mention the possibility of some officials‘ not reporting the money obtained from this crime as a suspicious transaction in exchange for bribery. The technical reasons may be individuals‘ not sharing their private bank information and other technical problems stemming from the codes of each country. If the information flows are delayed or absent due to corruption, it may be possible to increase institutionalization through FATF and similar organizations in the relevant countries and prevent corruption. If the size of the corruption is very large and the administrative weaknesses of the countries concerned, the implementation of the above-mentioned sanctions by FATF and the international community may be the solution to the problem. In the case of technical problems, the solution of this problem with the help of international cooperation and organizations such as FATF can be possible only with the sincere will of the countries concerned.

Inadequate Legal Assistance Between Countries: The technical aspect of the problem comes to the fore in the poor functioning of mutual legal aid processes. The ratification of international conventions under legal aid by all countries and, more importantly, their implementation without

reservation to any convention clause is of vital importance in this struggle. If the place where the offense is committed and the place of the perpetrator are different, the functioning of an effective trial process will be prevented in case the reservation is made to the convention. In order to solve this problem, especially the UN and related international institutions and organizations may draw attention to the damages caused by terrorism and human trafficking to the international community and human dignity. Thus, by the pressure of the international community, the countries which are inadequate in legal aid can participate in the conventions or fulfill the requirements of the conventions to which they are a party. In addition, the fight against human trafficking may be interrupted as a result of exceptional circumstances where the legal aid processes operated on human trafficking may be inadequate. It is not possible to add any exceptions to the contracts that may arise in relation to the crime of human trafficking. However, the framework in the context of judicial assistance can be further expanded with additional special contracts between countries with the heaviest traffic.

Poor Border Controls Between Countries: It can be argued that one of the most important problems in the fight against human trafficking is weak border controls. The reason for this may be the weak border controls stemming from the unstable structure of the Middle East and North Africa, especially when compared to the rest of the world. This fragile structure of the Middle East and North Africa region creates a very productive environment for human trafficking. This fragile structure of the Middle East and North Africa region creates a very productive environment for human trafficking. Due to this unstable structure, border controls, cross-border cooperation and coordination remain weak in the region. Initiatives to prevent organized crime, such as human trafficking, require strong and effective controls on the borders of countries. Considering the urgency of this problem, countries in the region may take steps to prevent the crime of human trafficking that disregards human dignity. In order to achieve this, the humanitarian dimension of the issue can be emphasized and joint studies can be conducted under the leadership of the UN to increase border controls in the countries with the heaviest traffic. Providing technical, logistical and financial support to such countries within the scope of these joint activities will encourage them to take measures related to border controls. However, it is much more difficult to solve the problem, especially in countries where some of the territories close to the border are under the control of various terrorist organizations. It is not possible for measures to be taken and border controls to be made in the context of human trafficking until these regions are free of terrorism and controlled.

As a result, regarding the solution of the topics of inadequate sharing of intelligence, inadequate mutual assistance and weak border controls between countries, it is crucial that the problematic countries are increasingly and more powerfully directed, encouraged and suppressed by the international community, that sanctions are imposed and some are imposed collectively. With increasing international pressure, it will be possible to achieve results in this struggle. Hence, Iran was also oppressed in the Iranian Nuclear Crisis and was forced to reach an agreement as a result of long efforts. In the current struggle, incentives, suppression and sanctions are applied, but this is not enough. International incentives, support and increasing pressure continue to be of great importance in this struggle.

BIBLIOGRAPHY

Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, "MALİ EYLEM GÖREV GÜCÜ, YAPTIRIM MEKANİZMASI", (http://www.uhdigm.adalet.gov.tr/fatf/yaptirim_mekanizmasi.html), Access: April 29, 2019.

BBC, (2014) "Islamic State: Yazidi women tell of sex-slavery trauma",(https://www.bbc.com/news/world-middle-east-30573385), Access: April 20, 2019.

Council of Europe, Parliamentary Assembly, Committee on Political Affairs and Democracy, "Funding of the terrorist group Daesh: lessons learned", (http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24506&lang=en), Access: May 23, 2019.

Egmont Group, "About", (https://egmontgroup.org/en/content/about), Access: April 19, 2019.

Erdal, Hakan, (2008) "Organize Bir Suç Türü Olarak İnsan Ticareti ve Türkiye Örneği", Polis Bilimleri Dergisi, 10, 2, p. 79-90.

EUROPOL, (2011) "EU Terrorism Situation and Trend Report 2011", Report.

FATF Report, (2018) "Financial Flows from Human Trafficking July 2018", (https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf), Access: April 26, 2019.

FATF Report, (2015) "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)",(http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf), Access: April 22, 2019.

FATF Report, (2011) "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants July 2011", (https://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf), Access: April 17, 2019.

Gürel, Selahattin, (2015) "Terör ve Terör Örgütlerinin Finans Kaynakları", Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi, 2, 4, p. 15-27.

Mali Suçları Araştırma Kurulu, "VİZYON & MİSYON", (http://www.masak.gov.tr/tr/content/vizyon-misyon/38), Access: May 12, 2019.

Mullins, Sam, and James K. Wither. "Terrorism and Organized Crime." *Connections*, vol. 15, no. 3, 2016, pp. 65–82. *JSTOR*, www.jstor.org/stable/26326452.

NATO, (2007) "Kötülüğün Kökündeki Para: Milletlerüstü Terörizmin Ekonomisi", (https://www.nato.int/docu/review/2007/issue2/turkish/analysis2.html), Access: March 22, 2019.

Organization for Security and Co-operation in Europe, "Leveraging Anti-Money Laundering Regimes to Combat Trafficking in Human Beings", (https://www.osce.org/secretariat/121125?download=true), p. 21, Access: October 17, 2019.

Özdek, Yasemin, (2009) "Küresel Yoksulluk ve Küresel Şiddet Kıskacında İnsan Hakları", (http://www.muharrembalci.com/hukukdunyasi/alintilar/509.pdf), Access: March 22, 2019.

Polis Akademisi Yayınları, (2018) "İnsanlığa ve Demokrasiye Terör Tehdidi: PKK Örneği", (https://www.pa.edu.tr/Upload/editor/files/PKK_Ornegi_Raporu_TR.pdf), Access: April 12, 2019.

Sarı, İsmail, "The Nexus Between Terrorism and Organized Crime; Growing Threat?", (https://dergipark.org.tr/tr/download/article-file/155620), Access: October, 22, 2019.

Statista, (2019) "Nearly A Third Of Human Trafficking Victims Are Children", (https://www.statista.com/chart/16719/detected-victims-of-human-trafficking/), Access: May 5, 2019.

Statista, "Human trafficking - statistics and facts", (https://www.statista.com/topics/4238/human-trafficking/), Access: May 10, 2019.

The Financial Action Task Force, "2017-2018 Annual Report", (http://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF-annual-report-2017-2018.pdf), Access: May 26, 2019.

The Financial Action Task Force, "History of the FATF", (http://www.fatf-gafi.org/about/historyofthefatf/), Access: May 13, 2019.

The Financial Action Task Force, "Countries FATF members", (https://www.fatf-gafi.org/countries/#FATF), Access: May 10, 2019.

The Financial Action Task Force, "Who we are", (http://www.fatf-gafi.org/about/), Access: May 13, 2019.

Türkiye Cumhuriyeti İçişleri Bakanlığı, "PKK, Bir İnsan Kaçakçılığı ve Uyuşturucu Ticareti Örgütüdür", (https://www.icisleri.gov.tr/pkk-bir-insan-kacakciligi-ve-uyusturucu-ticareti-orgutudur), Access: May 18, 2019.

United Nations, (2019) "Identifying and Exploring The Nexus Between Human Trafficking, Terrorism, and Terrorism Financing", (https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf), Access: April 26, 2019.

United Nations, (2018) "Report of the Secretary-General on Conflict Related Sexual Violence", (https://www.un.org/sexualviolenceinconflict/wp-content/uploads/report/s-2018-250/SG-REPORT-2017-CRSV-SPREAD.pdf), Access: April 22, 2019.

United Nations, (2015) "Transforming our world: the 2030 Agenda for Sustainable Development", (https://sustainabledevelopment.un.org/post2015/transformingourworld), Access: April 10, 2019.

United Nations, (2014) "Security Council S/2014/770", (https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_770.pdf), Access: April 24, 2019.

United Nations, (2014) "Security Council S/2014/815", (https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2014_815.pdf), Access: April 22, 2019.

United Nations, (2000) "PROTOCOL TO PREVENT, SUPPRESS AND PUNISH TRAFFICKING IN PERSONS, ESPECIALLY WOMEN AND CHILDREN, SUPPLEMENTING THE UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME",(https://treaties.un.org/doc/Treaties/2000/11/20001115%2011-38%20AM/Ch_XVIII_12_ap.pdf), Access: April 19, 2019.

United Nations, (2018) "The nexus between human trafficking and terrorism",(https://www.un.org/sc/ctc/wp-content/uploads/2018/11/2.-Ms-Delphine-Schantz-CTED.pdf), Access: October, 20, 2019.

United Nations Office on Drugs and Crime, (2018) "Global Report on Trafficking in Persons 2018",(https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf), Access: April 14, 2019.

United Nations Office on Drugs and Crime, "Combating Illicit Trafficking, Organized Crime and Terrorism", (https://www.unodc.org/middleeastandnorthafrica/en/regional-programme-framework/trafficking-crime-and-terrorism/trafficking-crime-and-terrorism.html), Access: May 10, 2019.

United Nations Office on Drugs and Crime, "Human Trafficking", (https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html), Access: May 10, 2019.

The United Nations Office on Drugs and Crime, "What are the root causes of trafficking?", (https://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_9-2.pdf), Access: October 19, 2019.

This Page Intentionally Left Blank

DATR, 2019; 12 : 29-43

ISSN 1307 - 9190

Methods of Martyrdom: Examining Changing Targeting Patterns in Suicide Attacks Towards Non-Democratic States

Jakob Urda[1]

Abstract**:** *Suicide attacks are more lethal and difficult to deter than their conventional counterparts. However, despite their destructive potential, suicide attacks only make up between one and five percent of overall terrorist attacks.*[2] *Literature around suicide attacks has established a series of conditions that have been thought necessary for the germination of a suicide terror campaign. Among these conditions is that the occupier be a country with a democratic government. From 1980 to 2003, nearly every suicide campaign involved a target nation which had democratic institutions. This article argues that this longstanding relationship no longer holds true. Today, almost every suicide campaign targets a country which has limited or nonexistent political liberty. This paper uses three decades of Freedom House data to show that democratic institutions are no longer necessarily the primary targets of suicide terrorism, and offers explanations as to why.*

Keywords**:** *suicide terrorism, insurgency, martyrdom, Pape, bombing*

1 The Author is Jakob Urda. Jakob was the Senior Suicide Attack Data Analyst at the Chicago Project on Security and Threats and worked to maintain the Suicide Attack Database (SAD). He has lectured for COE-DAT on suicide terrorism. Jakob has produced research for work in the Journal of Policy and International Affairs, SAGE, the Takshakshila Institute, and Hudson Institute. The views of the author do not necessarily express the views of the organization.

2 Robert Anthony Pape. *Dying to win: the strategic logic of suicide terrorism*. New York: Random House Trade Paperbacks. 2005.

This article examines trends surrounding suicide attack targeting. Specifically, it looks at the pattern of terrorist groups targeting states with democratic governments versus states with authoritarian governments. Situating this change in attack patterns is crucial for understanding suicide attacks as a phenomenon and their role in modern insurgency. This is because scholarship argues that the decision to target countries with democratic governments, which has traditionally characterized suicide campaigns, informs the strategic logic of suicide terrorism. Targeting democratic institutions is seen as a necessary and causal element of terrorist strategy; this means that any changing patterns of insurgent behavior require interrogation and rationalization.

Understanding the development of suicide attack behavior is important for addressing some of the most violent conflict zones in the world. The scope of suicide terrorism has widened dramatically since the earliest examples of modern suicide campaigns in the 1980s. From an average of fewer than ten attacks per year during the 80s, there are now hundreds of attacks a year. In 2015, there were 653 suicide attacks across the world, an all-time high.[3] As a tactic, suicide terrorism is employed in many of the world's deadliest environments: from Syria to Afghanistan to Nigeria. The six conflicts which the Global Terrorism Database terms 'most impacted by terrorism' – Syria, Iraq, Afghanistan, Nigeria, Somalia, and Pakistan – are see major incidences of of suicide terrorism.[4] Many of theatres impacted by suicide terror such as Syria, Afghanistan, and Somalia, also show few signs of resolution.

Any changes in suicide attack patterns since their origin in the 1980s should prompt scholarship to revisit the theory around the tactic. This paper will use a time-series analysis of data collected by Freedom House over the last three decades to argue that suicide terrorism is increasingly targeting states with non-democratic governments. Shifting patterns of terrorist behavior may reveal new insights about the strategic logic of suicide terrorism or challenges to long held assumptions. The puzzle is therefore *whether the characteristics of countries targeted by suicide attacks has changed, and if so, why?*

Why Suicide Attacks?

Within insurgent tactics, suicide attacks bear special significance for study. By magnitude, suicide attacks kill far more people per attack than conventional terrorism – twelve per attack versus one, respectively.[5] Suicide attacks have also posed particular problems for counterinsurgents and security operatives, because they are so hard to prevent and deter. Suicide attacks require no exfiltration and minimal self-defense for the attacker, rendering ineffective most conventional means of deterring violence through the use of armed force. This is why suicide attacks are almost exclusively used in asymmetric conflicts, where suicide attackers use martyrdom to compensate for tactical disadvantages that they face against state actors.

From an academic perspective, studying suicide attacks is valuable because it sheds light upon the strategic logic of terrorist groups. Robert Pape of the University of Chicago writes that nearly 95 percent of suicide attacks on record have happened in a handful of organized campaigns, with specific political objectives. Suicide attacks rarely happen at random or in isolated circumstances. Despite

[3] Robert Anthony Pape. The Strategic Logic of Suicide Terrorism. The University of Chicago. American Political Science Review. August 2003.

[4] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Data file]. Retrieved from https://www.start.umd.edu/gtd

[5] Pape, Ibid.

making up nearly half of the overall deaths from terrorism, suicide attacks comprise less than 5 percent of total terrorist incidents.[6] The combination of the rarity of suicide attacks and their concentration in organized campaigns suggests that the circumstances where suicide terrorism is used are governed by a strict set of cross-sectional criteria. Therefore, understanding how changes in the targeting patterns of suicide attacks helps make clear the motivations and capabilities of terrorist groups.

Tactically, it is important to understand suicide attacks because terrorists face constant tradeoffs. The use of any particular tactic – for terrorists or otherwise – is the result of a group believing that this course of action is more likely to produce favorable outcomes than possible alternative tactics. Suicide attacks are hardly the most common or easiest form of insurgency to deploy; terrorist groups could opt for guerrilla tactics, political assassination, conventional civil war, nonviolent resistance, or any number of other tactics based on their cost benefit analysis of the situation at hand.[7] In fact, social taboos and the necessary death of the attacker ought to make suicide attacks unattractive options from the outset to most terrorists. Similarly, only a small set of political grievances can be resolved through armed resistance, let alone suicide terrorism. Therefore, studying the cases where suicide terror is used – and understanding the causal processes behind them – sheds light on the structure and selection of insurgent tactics.

Why Democracy?

Most of the targets of suicide terrorism have been countries with democratic governments.[8] By targets, we mean the nationality of the target, not necessarily the country where the attack was carried out. Thus, a suicide attack which killed an Israeli soldier in Lebanon would be said to have targeted Israel. Historically the targets of suicide terrorism have held competitive elections and offered a substantial degree of political liberty to their citizens. Before the American interventions in Iraq and Afghanistan, the states which were victims of the most suicide terrorism – Israel, Sri Lanka, Lebanon, India, Turkey, Russia, and the United States – could all be classified as democratic at the time. During this wave of suicide terrorism, the late 1980s through the 1990s, all of the countries targeted by suicide terrorists could reasonably be said to have democratic governments.[9] Even states which have historically fluctuated in their commitment to political liberty such as Russia were targeted by suicide terrorists during a period in their history when they held comparatively free and open elections.

The relationship between suicide attacks and countries with democratic governments speaks to the strategic logic of the terrorist groups perpetrating those attacks. Suicide attacks have previously targeted the soldiers of states with democratic governments, or their close allies.[10] Because the democratic quality of target nations is theorized to speak to the logic of terrorists who use suicide, any deviation or evolution in targeting patterns bears relevance for developments in global terrorism. We ought to be curious as to why the targeting of democratic states has changed, and examine the implications that this shift has for the theory surrounding suicide attacks.

---

6 Ibid.

7 Shapiro, Jacob N. *The Terrorist's Dilemma: Managing Violent Covert Organizations*. Princeton University Press, 2013.

8 Eric Chenoweth. "Terrorism and Democracy." Annual Review of Political Science Vol. 16. May 2013) https://doi.org/10.1146/annurev-polisci-032211-221825

9 Ibid.

10 Pape, Ibid.

The condition of states with democratic systems as the main targets of suicide terrorism is not merely incidental; it is often touted as a nigh-on essential condition. Robert Pape designed a Suicide Attack Database that catalogs every suicide attack publicly and on record. In Dying to Win, he uses this data to generate a framework for the necessary conditions for a suicide terrorist campaign. Pape highlights four key characteristics that increase the likelihood of suicide terrorism: (1) political struggles over the occupation of one territory by another country, (2) a background of religious differences, (3) the occupying nation is democratic, and (4) the conflict has a legacy of prior conventional-style terror attacks. His argument is that terrorists use suicide attacks in order to coerce the democratic occupying nations to withdraw from the contested territory. While this data cannot disaggregate the target of the suicide attack from the intended target, this research assumes that on the aggregate the nationality of the target is generally representative of the targeting logic of the attacker.

Pape argues that democracy is an important condition for suicide terrorism because terrorists believe that societies with democratic governments are less cost tolerant than autocratic ones. That is to say, terrorists believe that when faced with high casualties, costs and the credible threat of more attacks to come, democratic governments will give in to their demands. The argument is that suicide attacks are a form of coercive punishment. By themselves, terrorist groups are unlikely to secure battlefield victories against more powerful military forces. Instead, they hope to generate pressure and costs for occupiers in order to convince them that continued presence is not worth the price of occupation. For democratic governments, terrorists believe that dramatic, high cost attacks will tip public opinion against intervention and in favor of withdrawal.

This argument is supported by the logic that terrorists are responsive to tradeoffs. This means that suicide attacks will only be used in circumstances where terrorists reasonably think that it will actually help them achieve their political objectives. The theory argues that terrorists believe democratic governments are responsible to voters, who are less willing than dictators or oligarchs to tolerate heavy casualties. The differentiation in tactics is evident in the history of conflict in Afghanistan, where the mujahedeen never employed suicide attacks against Russian occupiers in the 1990s, whereas the Taliban eagerly used those tactics against American occupiers in the 2000s. Suicide terrorism exploits "the rationality of irrationality," in which the seemingly irrational and extreme martyrdom of suicide terrorists conveys credibility to a democratic audience that even more violent, undeterrable attacks will continue.[11]

The link between suicide attacks and democratic governments is evidenced in the history of successful political concessions gained following highly visible suicide attacks. In one of the most significant cases of suicide terrorism during the 1980s, Hezbollah militants in Lebanon targeted a US marine barracks, killing over 230 soldiers. The highly publicized attack was in retaliation for the intervention of American and French peacekeeping forces in Lebanon's multifront sectarian civil war. Soon after, President Ronald Reagan acknowledged the need to "make [American] forces less vulnerable to those who want to snipe at them or send in future suicide missions."[12] America withdrew from Lebanon shortly thereafter. Similarly, in 2004, a series of suicide bombings in Madrid successfully tipped the Spanish electorate from the incumbent Popular Party to the rival Socialist Party. The Socialist Party called for the removal of Spanish troops from the Iraq war, a move which

[11] Robert Pape. The Strategic Logic of Suicide Terrorism. The University of Chicago. American Political Science Review. August 2003.

[12] Ronald Reagan. Address to the Nation on Events in Lebanon and Grenada. Reagan Press Library. October 27, 1983

was opposed by the Popular Party. Spain exited the conflict only a few months later, a seeming validation of the use of suicide attacks to coerce democratic governments into withdrawal.[13]

One possible argument against the theory that terrorists seek to exploit the low cost tolerance of democratic governments is that they are not actually less tolerant than autocracies. Many argue that states with democratic institutions seem willing to bear heavy burdens and sustain dramatic costs, especially when core security interests are at stake. The American war in Vietnam lasted 17 years, costing billions of dollars and 50,000 combat casualties, while Britain sustained 450,000 deaths during World War II. In fact, even absent the argument about democracies specifically, many scholars note skepticism over the logic of coercive punishment in general. Modern states are incredibly resilient, especially when faced with external military threats. Literature on strategic aerial bombing has found that civilian punishment is generally ineffective because the fear of coercive punishment is more often outweighed by the unifying effect of increased nationalism and shared struggle.[14]

However, an important element of terrorist coercion is not the actual cost tolerance of democratic states, but the perceived cost tolerance. Regardless of the actual willingness by democratic governments to sustain casualties, the argument goes that terrorists believe that societies which are ruled by voting civilians are less likely to stomach the violence of suicide terrorism.

Methodology

Comparative analysis requires that we split up the timeline of suicide terrorism into reasonable subunits, or phases. This allows us to compare different periods where suicide attacks are qualitatively different and examine the changes in suicide attack behavior. This is akin to comparing other continuous time-series phenomenon by creating analytical boundaries. For instance, many studies of the Cold War divide the conflict into distinct periods based on the changing relevancies. This paper will use the work of Robert Pape and James Piazza in order to classify the successive waves of suicide attacks.[15]

The first phase of suicide attacks occurred between 1980 and 2003, and represents the beginning of the use of the tactic. This phase began with the deployment of suicide attacks in Lebanon against American armed forces and continued against Israel, Sri Lanka, India, Turkey, Russia, and the United States. This cluster of suicide attacks campaigns occurs in heterogeneous conflicts. It involves the invasion and occupation of neighboring countries, regional peacekeeping missions, and trans-hemispheric conflict.

The second wave of suicide attacks occurred roughly between 2003 and 2013. This phase is driven primarily by the US's Global War on Terror—from the invasions of Iraq and Afghanistan. This time period saw a dramatic increase in the volume of suicide attacks per year. The highest number of attacks of the first wave occurred in 2002 with 66 attacks, why by 2007 the number of annual suicide attacks had reached 522.

The final wave of suicide attacks happened after 2013. This time period captures two important trends in the landscape of suicide terrorism: first, the withdrawal of American forces from Iraq and

[13] James Phillips "Spain's Retreat After The Madrid Bombings Rewards Terrorism". Heritage Foundation. 3002.
[14] Pape, Ibid.
[15] Piazza, James A. 2008. "A Supply-Side View of Suicide Terrorism: A Cross-NationalStudy." Journal of Politics. 70(1):28-39.

Afghanistan and, second, the rise of ISIS. The exact date for withdrawal in Iraq is debatable (and had started much earlier), but by 2013 the United States had begun massive reductions in combat troops in Afghanistan. This distinction is analytically necessary because it represents a shift in the targets of the attacks in Iraq and Afghanistan from attacks against Americans to attacks against the local governments. Changing the exact year that this phase begins does not alter the conclusions that follow, because the democratic nature of the countries in question does not change over this period.

Some may argue that some campaigns of suicide terrorism happen in complex battlefields where identifying the target is difficult. They might also argue that suicide attacks in places like Syria are spillover from earlier conflicts against democracies such as Iraq. On the first point, it is true that the regimes in Iraq and Afghanistan do not exist independently of American support. However, it is fair to code the countries as non-democratic because suicide bombers no longer inflict direct costs in the form of casualties against American forces. Similarly, on the second point, the Syrian Civil War was certainly exacerbated by the conflict in Iraq, but suicide attacks in Syria no longer impose a direct cost for the United States. The theory being tested is whether or not the strategic logic of suicide terrorism is to inflict costs against countries with democratic systems. As such, for the purpose of the theory being tested, it is the local autocratic governments who bear the direct costs of suicide attacks.

The democratic institutions of target nations can be measured using Freedom House political liberty scores. Freedom House is a prominent NGO which tracks different metrics pertaining to democracy, economic openness, and other freedoms by country across time. Freedom House's methodology for collection is mostly consistent across time, which allows time series data to be compared effectively. While Freedom House collects statistics on many elements of freedom, the most relevant for this purpose is their score on political liberty. They examine political liberty with a series of ten political rights indicators applied uniformly across countries. The political rights indicators are grouped into three subcategories which allow Freedom House to analyze the openness of a state's institutions to its people: Electoral Process (3 questions), Political Pluralism and Participation (4), and Functioning of Government (3). Freedom House uses these questions to place countries on a scale between 1 and 7, with 1 being 'Free' and 7 being 'Unfree'.[16] The standards for collection and accuracy are also widely accepted within the academic community; prior research on suicide terrorism and democracy has often cited Freedom House data.

It is worth mentioning that civil war may impact the political liberty score by creating conditions where pluralism and normal government functions are more difficult. However, in the sample cases relevant to this research, such a bias is not a concern. All of the relevant countries maintain their scores throughout the three waves being analyzed, and the scores are taken at the beginning of the suicide terror campaigns. This means that the likelihood of reverse-causality is limited because there is little or no movement of the scores. The countries were coded as autocracies before the suicide campaigns were launched because they genuinely reflect the political characteristics of autocratic governments.

The data for suicide campaigns is drawn from Robert Pape's books, Dying to Win and Cutting the Fuse.[17] This paper uses Pape's list of suicide campaigns for two reasons. Firstly, these groupings of suicide terror are widely used among academics, with over five thousand academic citations, far more than other works on the topic. Because Pape's research on suicide terror campaigns was so

[16] "Freedom in the World." Freedom House International. January 2019.

[17] Pape, Robert A., and James K. Feldman. *Cutting the Fuse: The Explosion of Global Suicide Terrorism and How to Stop It*. University of Chicago Press, 2010.

seminal, it is useful and appropriate for future work which evaluates changes in suicide terrorism to reference his earlier models as a baseline. Second, Pape's framework for campaigns captures a wide portion of actual suicide terrorism. His campaign groupings account for between 80 and 95 percent of all worldwide suicide attacks and thus provide a strong starting point for clustering attacks together.

This paper conducts an observational study to see how the relationship between democracy and suicide terrorism has changed over time. This paper assesses this changing relationship in two ways: (1) a simple average of political liberty score of countries in each successive wave of suicide attack, and (2) a weighted average. The simple average uses the political freedom score of each country which was the target of a suicide attack campaign during the date range, while the weighted average considers which of those campaigns featured more attacks.

The simple average is useful because it provides a clear picture of the state of suicide attacks. This is the most straightforward answer to whether or not terrorists still prefer to target democracies. A result indicating that target nations are largely democratic would be consistent with previous works, while a digression would indicate the opposite. I will take the Freedom House scores of each country in a given wave of suicide terrorism—specifically, the score from the year when the suicide terror campaign began. Then, I will average the scores of countries within one wave and compare them to the scores of the other waves.

The weighted average is useful because it speaks to the logic of using suicide attacks. Weighting the political liberty score of states which experience larger volumes of suicide terror make sense because those are the states which terrorists have deemed more suitable targets. They may therefore better represent the strategic conditions under which suicide terrorism is successful. This method is accomplished by proportionally weighting each target of suicide terrorism by the volume of attacks directed towards them. Each attack represents an instance where a terrorist groups makes the strategic decision to use suicide attacks, so countries which are the target of more attacks ought to represent more favorable conditions for the tactic. This method allows us to see the conditions of the mean suicide attack, the 'most average' individual attack, and who it targets.

Data

Simple Averages

The first average involves the wave of suicide attacks between 1982 and 2003. During this period, Pape delineates suicide terror campaigns in Lebanon, Israel, Sri Lanka, India, Turkey, Russia, and the United States. The following table examines these 7 campaigns and their Freedom House Scores. The Freedom House scores correspond to the period when th*e target nation began to be attacked by suicide terrorists during the campaign in question.*

Table 1: Freedom House Scores and Corresponding Freedom Status

FREEDOM STATUS	**FREEDOM HOUSE SCORE**
FREE	1.0 to 3.0
PARTLY FREE	3.0 to 5.5
NOT FREE	5.5 to 7.0

Table 2: Simple Average for Wave I (1982-2003)

CAMPAIGN NAME	TARGET COUNTRY	FREEDOM HOUSE SCORE
LEBANON VS. COALITION	US, France, Israel	1, 1, 2
ISRAEL VS. PALESTINIAN GROUPS	Israel	2
SRI LANKA VS. LTTE	Sri Lanka	4
INDIA VS. BKI	India	4
TURKEY VS. PKK	Turkey	4
RUSSIA VS. SEPEARATISTS	Russia	5
UNITED STATES VS. AL QAEDA	United States	1
WAVE 1 AVERAGE		**2.66**

The average political freedom score for a target of suicide terrorism during the first wave is 2.7, far closer to 'Free' than 'Unfree.' Among these countries, not one of them would be considered 'Unfree' by the rankings, the lowest being 'Partly Free' Russia. The US and Israel feature twice because they are the targets of multiple independent campaigns. Even if this is corrected for though, the average only changes slightly to 3.5, which is still termed 'Free.'

The second wave of suicide attacks, between 2003 and 2013, occurred during the height of the American War on Terror. The suicide attack campaigns in Pakistan, Afghanistan, and Iraq, which made up over 75 percent of all suicide attacks globally, happened in response to American interventions in the Middle East.[18] This period exhibits a similar pattern as before, with targeting focused on democratic states. The United States is coded as the target of attacks in Iraq and Afghanistan because (1) Western troops represent a disproportionate share of suicide attacks in these countries and (2) the stated objective of these attacks was to force American withdrawal.

Table 3: Simple Average for Wave II (2003-2013)

CAMPAIGN NAME	TARGET COUNTRY	FREEDOM HOUSE SCORE
AFGHANISTAN VS. TALIBAN	United States	2
IRAQ VS. REBELS	United States	2
PAKISTAN VS. REBELS	Pakistan	6
WAVE 2 AVERAGE		**3.33**

Here, the trend of targeting democracies holds constant, mainly because of the overwhelming weight of the United States. It should be noted that even this score is generous towards authoritarians because many scholars see the suicide attack campaign in Pakistan as retaliation for the crackdown on militancy which was lobbied for by Americans, and spillover from the war in Afghanistan.

[18] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Data file]. Retrieved from https://www.start.umd.edu/gtd

The trend of targeting democracies abruptly reverses itself in the third wave of suicide terror, from 2013 to the present. This wave represents Iraq after the US exit, and Afghanistan after the NATO/ISAF drawdown. At this point in time, the primary targets of suicide attacks in both countries are the local regimes. The most visible occupier of territory is no longer America but the local governments. While America is still technically present in Afghanistan, nearly all the fatalities of suicide attacks are locals. The other campaigns in this wave are Nigeria, Yemen, and Syria.

The countries being targeted in the third wave resemble the second wave. As such the recoding of the target country between the two waves is responsible for much of the swing in Freedom House scores. It is therefore important to underscore the fact that changes in US force deployment around 2013 constituted a very real and significant change in the targets and objectives of suicide terrorists. By 2011, the United States had formally exited the war in Iraq – which had, at its height, 170,000 troops on the ground. By the start of 2014, the American-led ISAF mission had fallen from 140,000 to 50,000, and the coalition had ended major combat operations. Thus, 2013 marks a shift where the primary antagonists for local insurgents and terror groups are no longer an American occupying force, but rather the local regimes themselves.

Table 4: Simple Average for Wave III (2013-2018)

CAMPAIGN NAME	TARGET COUNTRY	FREEDOM HOUSE SCORE
NIGERIA VS. BOKO HARAM	Nigeria	3
IRAQ VS. REBELS	Iraq	5
AFGHANISTAN VS. TALIBAN	Afghanistan	5
SYRIA VS. REBELS	Syria	7
YEMAN VS. REBELS	Yemen	7
WAVE 3 AVERAGE		**5.4**

Here the average political freedom score is 5.4, which is 'Partly Free', verging on 'Unfree' (5.5). If other smaller suicide attack campaigns were included, such as Libya, the score would increase to over 5.5. This is a 2.07-point increase in score from the second wave, and a 2.4-point increase in score from the first wave.

Weighted Averages

The weighted average places additional emphasis on areas where more suicide attacks happen. In doing so, this metric helps avoid undue influence by outliers or smaller campaigns. In Waves 2 and 3, Iraq and Afghanistan see an overwhelming majority of the attacks conducted around the world. The weighted average allows researchers to consider that those climates that are especially prone to attacks, and observe how such emphasis changes the resultant pattern of terrorist targeting.

Table 5: Weighted Average for Wave I (1982-2003)

CAMPAIGN NAME	NUMBER OF ATTACKS	POLITICAL LIBERTY OF TARGETS
LEBANON VS. COALITION	31	1.33
ISRAEL VS. PALESTINIAN GROUPS	79	2
SRI LANKA VS. LTTE	71	4
TURKEY VS. PKK	20	4
RUSSIA VS. SEPRATISTS	15	5
UNITED STATES VS. AL QAEDA	7	1
INDIA VS. REBELS	7	4
AVERAGE ACROSS CAMPAIGNS		**2.92**

Table 6: Weighted Average for Wave II (2003-2013)

CAMPAIGN NAME	NUMBER OF ATTACKS	POLITICAL LIBERTY OF TARGETS
IRAQ VS. REBELS	1157	2
AFGHANISTAN VS. REBELS	664	2
PAKISTAN VS. REBELS	289	6
WAVE 2 AVERAGE		**2.50**

Table 7: Weighted Average for Wave III (2013-2018)

CAMPAIGN NAME	NUMBER OF ATTACKS	POLITICAL LIBERTY OF TARGETS
NIGERIA VS. BOKO HARAM	349	3
IRAQ VS. REBELS	1709	5
AFGHANISTAN VS. REBELS	705	5
SYRIA VS. REBELS	304	7
YEMAN VS. REBELS	162	7
WAVE 3 AVERAGE		**5.07**

A weighted average of suicide attacks also supports the argument that terrorists have increasingly targeted autocracies. The data is slightly different, in part because an increasing number of attacks happen in Iraq during this period. Yet the results are still conclusive: a 2.16-point change from the first wave to the third, and a 2.57 change from the second wave. Before 2003, nearly every single target of suicide terrorism could reasonably be classified as democratic, holding competitive elections and boasting civilian control of government institutions. Only one, Russia, could be called Non-Democratic. By 2018, the pattern had reversed. Only a single major suicide terror campaign – Boko Haram against Nigeria – can reasonably be argued to be targeting a state with generally

democratic institutions. Even this outlier sits closely to the 'Partially Free' distinction with relatively young democratic institutions.[19]

Analysis and Discussion

The Freedom House data demonstrates that suicide attacks now primarily target authoritarian governments. This raises the question of why this shift has taken place, and what the implications are for existing theory. There are three explanations which comply with existing literature that might explain the growth in suicide attacks against non-democracies: (1) the weakness of modern autocratic targets, (2) the diffusion of the learning about suicide attacks, and (3) the development of suicide attacks as a tool of conventional insurgency. Terrorists still want to use suicide attacks against targets with low cost tolerance because they believe those circumstances will produce the most favorable results. The reason more autocracies are being targeted may be that terrorists increasingly believe that dictators – under the right circumstances – can be just as cost averse as democratic governments.

The contemporary autocratic targets of suicide attacks are countries that terrorists might believe share the low-cost tolerance of democratic societies. From Tables 2 and 5 we see that that suicide terrorists have traditionally targeted countries with democratic governments. Terrorists have targeted democratic states because they believe that governments that are elected by the people are not willing to tolerate high casualty numbers. However, elections are not the only factor which influences cost tolerance. A wide range of factors from the popularity of a regime to economic stability may influence a government's willingness to bear costs. Of course, this means that there are circumstances in which autocracies are risk averse and unwilling to bear costs as well; Francisco Franco's Spain declined to provide the full amount of material support requested by the Axis powers during World War II because of a fear that it would cause popular unrest in Spain. This is because, at least on some level, autocracies also need to court public support.[20]

Based on the data from Tables 4 and 7, terrorists likely infer that certain autocracies make for good targets of coercion based on a clearly demonstrated state weakness. If the logic for targeting states with democratic governments is that elections are a clear signal of low-cost tolerance, the particular autocracies targeted by suicide terrorism must make particular high visibility signals to show themselves as similarly averse to bearing costs. As democracies have made for the lion's share of suicide targets, only autocracies that communicate a significant level of fragility should qualify becoming the targets of attacks in the view of the terrorist group's leaders.

The autocracies that are subject to suicide terrorism have established themselves as amongst the most brittle and cost intolerant in the world. Afghanistan and Syria are the clearest examples in this category. In Afghanistan, after the American drawdown of troops in 2013, suicide attacks have nearly universally targeted the sitting government, which Freedom House rates as 'Unfree'. Despite nominal elections, Afghanistan is rife with corruption and election fraud, and is accused by its own citizens of being an extractive oligarchy run on the behest of a small tribal elite cadre.[21]

---

[19] Omololu Fagbadebo. "Corruption, Governance and Political Instability in Nigeria." African Journal of Political Science and International Relations. Vol 1. November 2007.

[20] G. Tullock. *Autocracy.* Springer Science & Business Media. December 6, 2012.

[21] "Why Afghanistan's government is losing the war with the Taliban." The Economist. May 2019.

It is unlikely that the Taliban use suicide attacks against the Afghan government because they hope that the Afghan electorate will push the government to withdraw from contested territory. The Taliban seek to control all of Afghanistan, a concession the government cannot make, and seek to topple the regime. The data shows that Afghanistan and America have essentially opposite Freedom House scores, yet suicide attacks have continued long after the American drawdown. Therefore, the normal logic of coercing democratic government would not seem to apply.

The Taliban target the Afghan government with suicide attacks because the Afghan government has demonstrated an inability to tolerate large costs, independent of a democratic government. Afghanistan routinely tops the list of the Fragile States Index, and outside speculators consistently rate it as being at high risk of collapse.[22] Despite billions of dollars in funding and an army of hundreds of thousands, the Afghan government has been unable to establish rule of law across the country. The Taliban control or contest about half of all the territory in Afghanistan.[23] Taken together, these highly visible signs of internal weakness satisfy the terrorist desire to coerce actors with low cost tolerances. The clearly demonstrated weakness of the Afghan government illustrates how the Taliban's use of suicide attacks follows the logic of coercion despite the undemocratic character of Afghanistan.

The logic of coercing weak autocracies is even clearer in Syria. The Syrian government has been the target of Islamic State suicide attacks since 2013 despite being a clear dictatorship, with the lowest possible Freedom House ranking for political liberty. Iraq, a frequent target of suicide attacks, also fares poorly on the Political Liberty Index. Nevertheless, both countries see a disproportionate number of suicide attacks against regime forces. The answer is similar to that in Afghanistan. Syria and Iraq have demonstrated high visibility state weakness over the last decade. The Syrian military has barely held its ground and only now begun to recover from a massively destructive, multifront civil war. The Iraqi Army melted away from ISIS during their initial confrontations, ceding its second largest city, Mosul, to the terrorists.[24] Both countries have been embroiled in conflict for so long and fared poorly against insurgencies for so long that it is reasonable to conclude that they would not be tolerant of high costs.[25] This has been born out over the course of the conflict. The Syrian government made the decision to largely ignore ISIS and allow other actors to focus on defeating them – the Assad regime instead chose to focus on taking back territory from other enemies (ones who did not employ suicide attacks to the extent of ISIS).[26]

The second reason why suicide attacks may now be used more frequently to target autocracies is because intergroup learning and highly visible success has facilitated a diffusion of the technology and tactics required for suicide attacks. As early documented successes of suicide attacks spread, terror groups may have become more willing to use the tactic in new circumstances. This has led to experimentation with suicide attacks in new scenarios, like autocracies.[27] For instance, the Taliban were initially resistant to using suicide attacks because of religious prohibitions on self-harm, but became convinced to deploy the tactic after seeing its success in Iraq.[28] Al Qaeda advisors who

22 "Fragile States Index 2019." Fund for Peace. April 2019.
23 Roggio, Bill. "Mapping Taliban Control in Afghanistan." Foundation for the Defense of Democracies. September 2018.
24 Joby Warrick. *Black Flags: The Rise of ISIS.* Anchor Books. 2016.
25 Price, Roz "Iraqi State Capabilities," K4D Helpdesk Reports. Institute of Development Studies, 18 May 2018.
26 Hendawi, Hamza and Abdul-Zahra, Qassim "ISIS Top Brass is Iraqi Army's Former Best and Brightest," Haaretz News. August, 2015
27 Gunaratna, Rohan, "Global Threat Forecast," Counter Terrorist Trends and Analyses. January 2018.
28 Williams, Brian Glyn. "Mullah Omar's Missiles: A Field Report on Suicide Bombers in Afghanistan". Middle East Policy Council. Winter 2006.

pioneered suicide attacks in Iraq helped convince the Taliban to adopt the tactic, and taught them how to use it successfully. Similarly, it stands to reason that the Islamic State's use of suicide attacks against the Syrian government follows from their demonstrated success in using the tactic against Iraqi forces in its earlier form, al-Qai'da in Iraq (AQI). The knowledge of how to carry out suicide attacks has widely been disseminated. Al Qaeda and ISIS both sport vast networks which are capable of inducting newer regional affiliates into their ranks and teaching them how to use suicide attacks. Indeed, ISIS deployed this tactic in Sri Lanka, bringing their institutional knowledge to a small local affiliate thereby allowing them to kill hundreds in the Easter Bombings in 2018.[29]

The third explanation for the deployment of suicide attacks against autocracies is that the strategic logic of suicide attacks has expanded to include a broader set of tactical uses – namely deployment in conventional style battlefields. Specifically, ISIS has showcased the use of suicide attacks as part of a combined arms warfare battleplan, substituting artillery and armor with large Vehicle Borne Improvised Explosive Devices (VBIEDs).[30] This logic is remarkably different to traditional uses of suicide attacks, which have focused on coercive punishment – to inflict large costs on an enemy in order to coerce them into withdrawing. This is why suicide bombers have traditionally not participated in conventional confrontations. ISIS's design for suicide attacks reflects denial — to seize battlefield objectives and targets in a direct conventional-war style confrontation with government forces. Suicide attacks as a frontline weapon were an essential part of ISIS's capture of Ramadi, where they routed government forces by using heavy VBIEDs to shatter entrenched positions and sow discord among defenders.

Suicide attacks used under the logic of denial circumvent the requirement that the target have a democratic government. This is because these suicide attacks no longer hope to merely inflict costs; they aim to win battlefield engagements. As discussed earlier, the reason which traditional punishment-style suicide attacks are employed is because they can coerce democratic electorates. But the aim of suicide attacks on the battlefield is to seize and hold target objectives and defeat enemy forces. These differing goals are not linked to the democratic character of the target. Suicide attacks on the battlefield kill troops from autocratic states just as well as those from democratic states.

Conclusion

The fragmenting relationship between suicide attacks and states with democratic governments raises important questions about the strategic logic of terrorist groups. The data shows a dramatic swing in targeting practices from countries with democratic governments to those with authoritarian governments – from an average political freedom score of 2.66 (Free) to now 5.4 (Unfree). This implies a broad shift in the motivations and/or capabilities of terrorist groups. Targeting is a core aspect of insurgent strategy – when, where and who to attack forms the core of terrorist planning. Therefore, this undeniable swing in the preferences of terrorists from targeting countries with democratic governments to targeting those with autocratic governments merits thorough investigation.

A substantial school of literature suggests that terrorists use suicide attacks primarily against

[29] Mandhana, Niharika, Rob Taylor and Saeed Shah. "Sri Lanka Bomber Trained in Syria With Islamic State". Wall Street Journal. April 2019.

[30] Lou, Johnny and Patrick O'Connor. "Why ISIS Is Winning in Iraq." The Small Wars Journal. 2017.

countries with democratic governments. This is because terrorists, like other groups, face tradeoffs, and seek to use high risk tactics like suicide attacks only when such there is a high likelihood of success. Thus, the perceived high cost tolerance of autocratic governments has been seen to deter suicide attacks out of concern that they would simply be ineffective.

This research suggests that the historic link between states with democratic governments and suicide attacks no longer holds. Autocracies are now the main targets of terrorist groups using suicide attacks. Only a small fraction of contemporary suicide attacks, namely in Nigeria, appear to target democratic states.

This research implies that changes must be made to traditional theories surrounding suicide attacks. Specifically, a new strategic logic must be developed which accounts for suicide attacks against autocracies. Several possible explanations emerge: first, that the particular autocracies targeted by suicide attacks have signaled a high degree of weakness and low degree of cost tolerance. Second, that the success and knowledge behind suicide attacks has been more widely disseminated amongst terror groups over the last two decades, making them more accessible as a tactic. Third, that suicide attacks against authoritarian governments are focused on achieving battlefield success instead of coercive punishment, reducing the insurgent's need to target low cost tolerance governments. Scholarship will have to adapt and evolve in order to explain the rise of suicide attacks against non-democratic targets.

BIBLIOGRAPHY

Akram Hijazi, "A Journey into the Mind of the Salafia al-Jihadia: Al-Qa'ida as a Model,"Al-Quds Al-Arabi newspaper published in London, August 28 to 31, 2006 (four parts), Part Two: The Economy and the Theory of the Snake's Head.

Michael Horowitz and Dan Reiter, "When Does Aerial Bombing Work? Quantitative Empirical Tests, 1917-1999," Journal of Conflict Resolution 45 (April 2001): 147-173.

G. Tullock. Autocracy. Springer Science & Business Media. December 6, 2012.

Hendawi, Hamza and Abdul-Zahra, Qassim "ISIS Top Brass is Iraqi Army's Former Best and Brightest," Haaretz News. August, 2015

Kube, Courtney "The Taliban is gaining strength and territory in Afghanistan," NBC News. 30 January 2018.

Joby Warrick. Black Flags: The Rise of ISIS. Anchor Books. 2016.

Johnny Lou and Patrick O'Connor. "Why ISIS Is Winning in Iraq." The Small Wars Journal. 2017.

Pape et al. "The American Face of ISIS." Minerva Research Initiative. Accessed January 31, 2019. https://minerva.defense.gov/Minerva-News/News_Display/Article/1672468/the-american-face-of-isis/.

Pape, Robert A., and James K. Feldman. Cutting the Fuse: The Explosion of Global Suicide Terrorism and How to Stop It. University of Chicago Press, 2010.

Pape, Robert Anthony. 2005. Dying to win: the strategic logic of suicide terrorism. New York: Random House Trade Paperbacks.

Price, Roz "Iraqi State Capabilities," K4D Helpdesk Reports. Institute of Development Studies, 18 May 2018.

Pedahzur, Ami. Suicide Terrorism. Polity, 2005.

Powell, Jonathan. Terrorists at the Table: Why Negotiating Is the Only Way to Peace. St. Martin's Press, 2015.

Robert Pape. The Strategic Logic of Suicide Terrorism. The University of Chicago. American Political Science Review. August 2003.

Shapiro, Jacob N. The Terrorist's Dilemma: Managing Violent Covert Organizations. Princeton University Press, 2013.

START. "2016 Global Terrorism Index." February 2017. Accessed January 31, 2019. http://economicsandpeace.org/reports/.

Williams, Brian. "Mullah Omar's Missiles: A Field Report on Suicide Bombers in Afghanistan | Middle East Policy Council." Middle East Policy Council. Accessed January 31, 2019. https://www.mepc.org/journal/mullah-omars-missiles-field-report-suicide-bombers-afghanistan.

"Global Terrorism Index 2018." Vision of Humanity, Accessed January 31, 2019. http://visionofhumanity.org/reports/.

Gunaratna, Rohan, "Global Threat Forecast," Counter Terrorist Trends and Analyses. January 2018.

"Fragile States Index 2019." Fund for Peace. April 2019.

This Page Intentionally Left Blank

DATR, 2019; 12 : 45-58

ISSN 1307 - 9190

Ransomware, A Tool and Opportunity for Terrorist Financing and Cyberwarfare

Alan Brill and Eric Thompson[1]

Abstract: *It is not unusual to hear military organizations consider cybercrime, whether directed at organizations in the private or public sectors, as falling into the domain of law enforcement and criminal prosecution authorities. Given the increased sophistication of cybercriminals, the use of cryptocurrencies for payment and the difficulties in tracking perpetrators across physical, international borders, organizations traditionally responsible for law enforcement find themselves undertrained, underfunded and unable to respond effectively to the scale and scope of cybercrime issues.*

The tools and techniques used by commercial cybercriminals can easily be repurposed to serve the objectives of terrorist groups and nation-state actors. To that end, cyber groups such as APT38*,* Lazarus Group *and* Hidden Cobra*, are already believed to be closely aligned with nation-states. Malware and ransomware, currently used to cripple corporations, can also disrupt military and civil government operations, build fear in civilian populations and further the goals of anarchists, terrorist groups or adverse nation-states.*

In this article, the authors discuss how ransomware and other types of malware can be repurposed by terrorists and nation-states to disrupt military and civil government operations while providing a credible alternative perpetrator – cybercriminals. The exponential escalation in ransomware payments, which has resulted in a multi-level financial model of providing ransomware and malware as services, is also discussed. New financial resources can be used to train an ever-increasing number of front-line cyberthreat actors with the developers safely out of harm's way. More importantly, these services now provide terrorist groups, who otherwise would not possess the technical skill to carry out cybercrime, with a new set of previously unavailable weapons.

[1] Alan Brill is a Senior Managing Director and Eric Thompson is a Managing Director in the Cyber Risk practice of Kroll, a division of Duff & Phelps. Mr. Brill is also an adjunct professor at the Texas A&M University School of Law. They may be contacted at abrill@kroll.com and eric.thompson@kroll.com

The authors do not advocate for military and government anti-terrorist organizations to take operational control of civilian anti-cybercrime operations. Defending non-military government agencies and corporations fall to private-sector cybersecurity vendors/consultants. Enforcement of civilian cybersecurity laws is, appropriately, the responsibility of law enforcement and criminal prosecution agencies. This is an area where inter-agency cooperation and information sharing will need to be improved as malware continues to morph into terrorist support software, herein described as "terrorware."

Keywords: cybercrime, cyberdefense, cybersecurity, cyberterrorism, cyberwarfare, ransomware

Ransomware is a subset of malicious software (malware) which encrypts files on a target workstation or network server for the purpose of extorting a ransom payment from the data owner. Dating back to 1989[2], ransomware attacks have grown in sophistication and danger. Modern ransomware, requiring bitcoin or other designated virtual currencies for payment, is traced back to CryptoLocker in 2013[3]. Until recently, ransomware infections were more commonly quick attacks. To stay ahead of traditional signature-based anti-virus (AV) software, ransomware attacked quickly and executed the payload, thus encrypting the targeted data before virus signatures could be updated to recognize and intercept it. The more advanced polymorphic malware, which can modify the structure of the malware dynamically, circumvents the majority of signature-based AV software, allowing the threat actor to adapt the kill chain (the series of events and particular versions of malware employed in a particular attack). It also enables the threat actor to use a combination of time and covert surveillance to cross laterally through a network and identify targets that will significantly increase the financial value of a ransomware attack.[4]

> *Cybercriminals, both organized criminal groups and Nation State Advanced Persistent Threat actor groups have been raising the stakes. […] In recent months, banking Trojan variants such as Emotet, Trickbot, ICE-ID, Qakbot, and others have been crippling companies, schools and government networks around the world. The newest strains don't stop at bank-related fraud; some join with other malware as secondary and tertiary payload drops into infected networks to saturate victims with unauthorized remote access looking for additional information to steal and can severely disrupt business. Some infected victims become part of a larger botnet and in recent months, Kroll has observed actor groups maturing their tactics and moving to deploy ransomware post network saturation as both a means to cover their tracks and to further monetize their intrusion through ransomware payments.*[5]

---

2 2019 marks the 30-year anniversary of the first ransomware attack. *PC Cyborg* (also known as the *AIDS Trojan,* because the target was AIDS researchers) was very basic and its ransom payment mechanism required the victim to mail a physical check to an address in Panama.

3 Liska, Allan. "Early Findings: Review of State and Local Government Ransomware Attacks." Accessed on May 10, 2019 at https://www.recordedfuture.com/state-local-government-ransomware-attacks/

4 Taking days or weeks to gather network intelligence allows threat actors to identify IT backup processes and backup storage locations. Threat actors can vastly increase the amount of a ransom if they are successful at destroying an organization's backups before detonating the ransomware executable.

5 Ackerman, Devon. "Evolving World of Cybercrime – Banking Trojans and Ransomware Deployment." Accessed on May 19, 2019, at https://www.kroll.com/en/insights/publications/cyber/cybercrime-banking-trojans-ransomware

Modern malware campaigns can run for weeks, months or years. In a major data breach involving a hotel chain, threat actors spent four years harvesting up to 500 million guest records. Threat actors observing the organization's network learn the routines of employees and IT staff, identify how they manage backups and understand the network defenses. By the time ransomware detonates, carrying out the encryption, threat actors will have already exhausted all options to move laterally through the organization's network, exfiltrate data, destroy backups, escalate privileges, deploy payloads and take control of network resources such as the Active Directory.[6]

In their work, the authors see cases in which hundreds to thousands of computers within an organization are compromised and have their files simultaneously encrypted when the threat actor detonates the ransomware executable files. In situations where the company or government agency does not have ransomware-hardened backups, a cyberattack may render the organization unable to operate or recover; consider how that capability can further the ends of both terrorist groups and nation-state actors. With increased sophistication, threat actors behind the ransomware variants such as Ryuk, Sondinokob and Dharma/CrySIS have exponentially increased demands[7], moving ransomware from an IT nuisance to a material threat to corporations, municipalities or a nation's operational security.

In recent months, there have been a series of highly targeted attacks on municipal systems around the United States. The number of towns and cities hit with ransomware attacks has increased exponentially. Through the end of September 2019, there have been 81 attacks against 230 municipalities as compared to 55 total attacks in 2018. "There have also been a couple of significant changes in attack methodologies during the year. The first is the series of attacks in Texas, which affected 22 municipalities. This attack is unique in that it represented the first ransomware attack against a state or local government where the attacker used a managed service provider[8] (MSP) as the entry point."[9] The attack, which deployed the Sodinokibi (REvil) ransomware, is consistent with other attacks which have relied on MSPs as their point of entry. Generally, cities and school districts have no choice but to pay the ransom demanded in hope that the criminals behind the attacks will provide a working decryption key in response.[10]

Ransomware attacks have become highly profitable. For example, the town of Lake City, Florida, reportedly paid a ransom of approximately US$460,000, surrendered through a transfer of 42 bitcoins to an anonymous virtual wallet,[11] to regain access to its files. In a similar attack, attributed to opening an attachment to a malware-bearing email, the files of the city of Riviera Beach, Florida,

6 Active Directory (AD) is a directory server which provides authentication and authorization mechanisms as well as a framework within which other related services on the network can be deployed (i.e., a network's central nervous system). Control of AD allows access to all network data and resources.

7 Fokker, John, & Mundo, Alexandre. "Ryuk Ransomware, Exploring the Technical and Human Connections", February 2019. Retrieved from https://www.coveware.com/blog/2019/2/19/ryuk-ransomware-exploring-the-technical-and-human-connections

8 A managed service provider (MSP) is a company to which an organization outsources some or all their information technology services, with the objective of improving operations or reducing cost. MSPs often operate by providing access to resources through an internet connection. The resources, which are controlled by the managed service provider, are said to be "in the cloud."

9 Liska, Allan. "Update: New Findings in Ransomware Attacks on State and Local Government". Accessed on October 8, 2019 at https://www.recordedfuture.com/state-local-government-ransomware-attacks-update/

10 Fernandez, Manny, Sanger, David E., & Trahan Martinez, Marina. "Ransomware Attacks are Testing the Resolve of Cities Across America." *The New York Times*, August 22, 2019.

11 Dudley, Renee. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks." *ProPublica*, August 27, 2019. Accessed on October 8, 2019 at https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

were encrypted. Faced with the enormous and expensive task of attempting to re-create the files, the City Council of Riviera Beach voted to pay the ransom of 65 bitcoins, with a then-current value of approximately US$600,000.[12] The potential cost of reconstruction was demonstrated when the city of Atlanta, Georgia, refused to pay a ransomware demand of US$51,000. According to published reports[13], Atlanta spent approximately US$17 million on recovery. The city of Baltimore, Maryland, refused a ransom demand of roughly US$76,000 and was reported to have spent more than US$5 million on initial recovery activities, with an estimate putting "the combination of lost revenue and city expenditures at more than $18 million."[14]

Given the cost of recovery, ransom payments measured in the hundreds of thousands of U.S. dollars can seem very reasonable. This was the case in Jackson County, Georgia, which paid a ransom of approximately US$400,000. The County Manager of Jackson, Mr. Kevin Poe, was quoted as saying "They demanded ransom. We had to make a determination on whether to pay. We could have literally been down months and months and spent as much or more money trying to get our systems rebuilt. They've been on our system I guess a couple of weeks. They really plotted their attacks before they hit us. They totally crippled us."[15]

The use of ransomware has become a global issue, with reports of successful attacks appearing in every part of the world. In many cases, the targeted government or company does not want it known that they were attacked or that they paid a ransom, so reported cases should be recognized as only a subset of the actual successful ransomware incidents. Some corporations have paid ransomware demands in the millions of US$ in order to reclaim control of their data files. Published reports disclose that companies that don't agree to pay a ransom but choose to employ specialist firms claiming to be able to crack the encryption carried out by the ransomware may be fooling themselves. A report in *ProPublica* stated that at least two such firms made ransom payments to cybercriminals, obtained decryption keys and then claimed that they had developed them, receiving payments from their clients which exceeded the dollar amount of the paid-out ransoms.[16]

Ransomware Attribution: Is it Just Cybercriminals?

"In the race to determine who is behind an attack, research facts (the *What* and *How* questions) are often put aside to focus on attribution (the *Who* question). This pursuit is understandable yet fundamentally flawed. Attribution is crucial, but there will always be unanswered questions."[17] An analysis of ransomware incidents, including how the attacks occurred in both a technical and operational

[12] Kass, D. H. "Riviera Beach, Florida Ransomware Attack: City Pays $600,000." Published online on MSSPAlert.com. Accessed October 8, 2019 at https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/riviera-beach-florida-malware-attack/

[13] Fernandez *op. cit.*

[14] Ibid.

[15] Ford, Wayne. "Cyber attack forces Jackson County to pay $400K ransom." *The Athens Banner-Herald*, March 8, 2019. Accessed on October 8, 2019 at https://www.onlineathens.com/news/20190308/cyber-attack-forces-jackson-county-to-pay-400k-ransom

[16] Dudley, Renee, & Kao, Jeff. "The Trade Secret. Firms that Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers." *ProPublica*, May 15, 2019. Accessed on October 8, 2019 at https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

[17] Fokker, John. "*Ryuk* Ransomware Attack: Rush to Attribution Misses the Point." Accessed on January 09, 2019 at https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/

sense, indicates that they are increasingly sophisticated and considerable amounts of money are being extorted from victims. Conventional wisdom points the finger at criminals and criminal enterprises around the world. In the attack on Atlanta's computer networks, for example, two Iranian nationals were charged in a U.S. federal indictment. According to a related U.S. Federal Bureau of Investigation (FBI) document, the indicted individuals carried out ransomware attacks on "more than 230 entities," extorted US$6 million in ransom payments, and inflicted "an estimated $30 billion in damages to the affected public and private institutions."[18] Putting the facts of the case together required the cooperation of the FBI, the United Kingdom's National Crime Agency, England's West Yorkshire Police, the Royal Canadian Mounted Police and the Calgary (Canada) Police Service. Since these attacks tend to be multinational, investigations require multinational cooperation as well.

Terrorists are aware of ransomware. "The FBI and security researchers say paying ransom contributes to the profitability and spread of cybercrime and in some cases, may ultimately be funding terrorist regimes."[19] Not all cybercrimes are the responsibility of NATO. The Alliance is not a police organization. But an analysis of the situation regarding ransomware provides a justification for NATO – and particularly the Center of Excellence – Defense Against Terrorism – to understand these attacks and why they represent an attractive opportunity for terrorist groups and rogue states.

Ransomware attacks represent an opportunity for terrorists and rogue states to:

- Use them as a source of funding. Evidence suggests the infamous Lazarus Group, a hacking crew believed to be operating out of North Korea, was behind the hack on the Far Eastern International Bank (FEIB) in Taiwan.[20] The anonymizing nature of cryptocurrencies are beneficial to terrorist groups and Nation-State Advanced Persistent Threat (APT) actor groups.[21]
- Use variants of ransomware as a tool to encrypt evidence of exfiltration, thereby providing additional time to use strategic and tactical intelligence. Exfiltrated customer data can also be sold through the "dark web" to criminals who can exploit those credentials and identities. Ackerman has stated that his team "has observed actor groups maturing their tactics and moving to deploy ransomware post network saturation as both a means to cover their tracks and to further monetize their intrusion through ransomware payments."[22]
- Take advantage of the nature of ransomware – encrypting files to make them inaccessible to the authorized users – as a way for terrorist groups to carry out offensive cyber-operations. Simply using the tools of ransomware to lock an adversary's systems can cause havoc. In the cases of municipal governments cited earlier, recovery without payment of ransom could take months, and might never result in complete knowledge of what was in the

---

18 Federal Bureau of Investigation. "Ransomware Suspects Indicted: Iranian Men Charged with Deploying Damaging *Sam-Sam* Ransomware" November 28, 2018. Accessed on October 8, 2019 at https://www.fbi.gov/news/stories/iranian-ransomware-suspects-indicted-112818

19 Dudley *op. cit.*

20 Cimpanu, Catalin. "North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist", October 17, 2017 at https://www.bleepingcomputer.com/news/security/north-korean-hackers-used-hermes-ransomware-to-hide-recent-bank-heist/

21 Brill, Alan, & Keene, Lonnie. "Cryptocurrencies: The Next Generation of Terrorist Financing?" *Defense Against Terrorism Review, 6*(1), Spring & Fall 2014, pp. 7-30.

22 Ackerman *op. cit.*

encrypted files. Imagine a police organization that couldn't access files of stolen vehicles or persons for whom arrest warrants had been issued. The use of ransomware with no intention of ever providing decryption keys converts ransomware to "terrorware,"[23] a very effective form of offensive cyberwarfare.

- Take advantage of the difficulty of identifying who is behind the attack. Because of the characteristics of international criminal investigations, proving who is behind a ransomware/terrorware event, a process known as "attribution," can be next to impossible, confusing the issue when considering whether and where to carry out counteroperations.

Ransomware and Terrorist/Rogue State Funding

Writing for the *International Center for Counter Terrorism* in The Hague, Entenmann and van den Berg stated:

> There are various ways in which terrorist groups can you virtual currencies. Organizations may use the Dark Web for obtaining weapons, including traditional firearms, explosives, chemical or biological toxins, paying for these with virtual currencies. virtual currencies could also facilitate other illicit income activities by terrorist groups; there has been for instance an uptick in virtual currency demands during kidnapping for ransom, with kidnaping for ransom being a popular source of income also for terrorist organizations. Similarly, if terrorist organizations move toward more digital attacks or cyberterrorism, virtual currencies may become more useful to these organizations as they allow for the purchase of "digital weapons" such as malware. Obviously, virtual currencies are not crucial to any of these activities, but they could make these transactions easier than traditional card payments or bank transfers.[24]

Rogue states, which are subject to international financial sanctions, could also use virtual currencies as a means for obtaining hard currencies through interactions with both legitimate and underground financial exchanges. Nichols states that "North Korea has generated an estimated $2 billion for its weapons of mass destruction programs using 'widespread and increasingly sophisticated' cyberattacks to steal from banks and cryptocurrency exchanges, according to a confidential UN report seen by *Reuters*."[25]

Few have the programming skills necessary to develop the sophisticated software that is now in use to carry out ransomware events. Fortunately for terrorist and rogue-state actors, some of those talented programmers make their malware available to others, either based on a license fee or by allowing access to a Ransomware as a Service (RaaS) site. "One example of this can be found on the top-tier Russian forum, *Exploit*. The ransomware dubbed "Buran" has been offered for sale, with the seller claiming

[23] "Terrorware is malicious computer software, sometimes called a cyber weapon. It incorporates features of malware, spyware, viruses, trojans, worms, adulterated firmware, and ransomware. It is deployed for the purpose of disrupting infrastructure and/or safety and security systems of a nation state. The *Stuxnet Virus* is a good example." Retrieved from https://www.urbandictionary.com/define.php?term=terrorware

[24] Entenmann, Eva, & van den Berg, Willem. "Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?" November 1, 2018. Accessed October 8, 2019 at https://icct.nl/publication/terrorist-financing-and-virtual-currencies-different-sides-of-the-same-bitcoin/

[25] Nichols, Michelle. "North Korea generated $2B from cybercrime to fund nuclear weapons program: U.N. report." *Reuters*, August 5, 2019. Accessed October 8, 2019 at https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

it will work on every version of Windows from XP to 10, encrypt files without changing extensions, and delete restore points for the user. It is being sold for a few thousand dollars."[26] In addition, there are skills needed to properly carry out a sophisticated reconnaissance program that proceeds a major ransomware attack in order to "tune" the attack software to maximize the damage. In many cases, this pre-attack analysis enables the ransomware to not only attack and encrypt operational files, but to encrypt the backup files that an organization may count on to counter the effects of an incident.

Ransomware as a Cyber Obfuscation Tool

There is an assumption associated with ransomware that the goal of activation/detonation is financial gain. While in many cases the ransom payment is the end goal, the experience of the authors and many others in the field, indicates that ransomware is increasingly being used to obfuscate the target of a potentially higher value cyberattack. North Korea has several malicious cyber groups, believed by researchers to be state-sponsored, which are known by the global cybersecurity industry under the names APT37,[27] APT38, Lazarus Group, Bluenoroff and Andariel.[28] In the notorious cyberattack carried out in October 2017 by APT38 against the Taiwan's Far Eastern International Bank, "Taiwan's Criminal Investigation Bureau discovered five malware files left by the hackers, including two ransomware files BITSRAN.EXE and RSW72CE, as well as three malware files which are designed to infiltrate a network, gather information, and destroy evidence."[29] Results of this attack would have seen North Korea steal the equivalent of approximately US$80 million and use ransomware as a tool to destroy the indicators of compromise (IOC - different network patterns, unexpected configuration changes, etc.). Ransomware is only one of a long list of malware tools available to the threat actor. When a cyber attacker's strategy is to infiltrate an organization's network, they follow similar stages:[30]

1. **Reconnaissance:** Attackers gather intelligence through public sources such as a corporate website or Twitter. They scan for vulnerabilities in gateways (connections between an organization and the Internet) that can be exploited and map out areas of weakness.
2. **Weaponization and Delivery:** Most successful endpoint compromises come through a socially engineered phishing attack, redirection to a rogue web site or a brute force attack targeting a weakly secured RDP[31] or VPN[32] connection.

---

[26] Sette, Nichole, & Hanson, Scott, "Ransomware on the Rise," Kroll's the Monitor, Issue 8. Retrieved October 7, 2019 at https://www.kroll.com/en/insights/publications/cyber/monitor/ransomware-rise-monitor-issue

[27] Council on Foreign Relations. "This threat actor uses social engineering techniques to target companies in the chemicals, electronics, manufacturing, aerospace, automotive, and health-care sectors, as well as the South Korean government." Retrieved from https://www.cfr.org/interactive/cyber-operations/apt-37

[28] US Department of the Treasury. "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups." Retrieved September 13, 2019 at https://home.treasury.gov/index.php/news/press-releases/sm774

[29] Yan, Sophia. "US report says APT38 behind Taiwanese bank NT$1.8 billion cyberheist." *The Taiwan News*. Retrieved October 04, 2018 at https://www.taiwannews.com.tw/en/news/3544541

[30] Paloalto Networks. "How to Break the Cyber Attack Lifecycle." Retrieved from https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

[31] "RDP" or "Remote Desktop Protocol" is a standard originally developed by Microsoft which enables a user to connect to and use a computer through an Internet connection.

[32] "VPN" or "Virtual Private Network" is a method for establishing and using an encrypted connection between an originating computer and a destination computer through the Internet. It can be thought of as a secure encrypted pipeline protecting the communications between the user's computer and the VPN server on the other end of the connection. The VPN server can then route the data onto the Internet or into another network.

3. **Exploitation:** At this stage, attackers use an exploit kit[33] or a weaponized document[34] to gain initial entry to an endpoint in an organization.
4. **Malware Installation and Privilege Escalation:** The malware has escalated and usurps administrative rights by establishing communication with the command and control centers. Traditional malware writes code to a user folder and then executes that code. A more recent trend is for malware to write directly to the active memory of a computer, leaving little to no trace on the hard drive or solid-state storage device, resulting in what is referred to as a "file-less exploit."[35]
5. **Communication with Command and Control:** With malware installed, attackers can now control the endpoint computer from a command and control center. This allows the cyber attacker to scan the network for the organization's content management system server, backups, domain controllers and other valuable assets.
6. **Lateral Movement:** Cyber attackers use droppers (programs that can install specific pieces of malware) such as *Trickbot* or *Emotet* to deliver custom polymorphic malware[36] tailored to avoid anti-virus software and exploit specific network vulnerabilities. At this point, the adversary is establishing multiple connection points into the network, fortify their cyber foothold and lay down the ransomware payload.
7. **Action on the Objective:** With control, persistence and ongoing communication, the cyber attackers will move forward with data exfiltration, destruction of backups, disabling of critical operations, initiation of financial wire transfers, or creation of fear with the end-goal of extortion.
8. **Ransomware Detonation:** Ransomware detonation/activation is the final step in the malware cyberattack lifecycle. This is the point at which the threat actor reveals their presence and the extent of the cyber compromises. The threat actor, at this point, has exhausted all of the tools in their arsenal to exfiltrate data and move through the network. In this final step, the attackers can use encryption to cover all remaining tracks that might reveal the information that was stolen or any alternative attack objectives, along with increasing the difficulty of attack attribution.

Ransomware and Offensive Cyber Operations

Whether within the structure of a State-Sponsored Advanced Persistent Threat Groups (APT)[37] or as part of the cyber operations of a terrorist group, cyber warfare can be characterized as being either

[33] An "exploit kit" is utility software that facilitates launching a specific form of attack against a target system. The kit makes it easier for a perpetrator to carry out a range of attacks (called "exploits") against vulnerabilities in the targeted system.

[34] A weaponized document is a document modified to facilitate an attack. It may contain, for example, a link to an infected website or have an attachment with malicious content.

[35] Kujawa, Adam. Director of Malwarebytes Labs. "Under the Radar – The Future of Undetected Malware." Retrieved from https://resources.malwarebytes.com/resource/under-the-radar-the-future-of-undetected-malware/?utm_source=blog&utm_medium=post&utm_campaign=q4fy19

[36] "Polymorphic malware is a type of malware that constantly changes its identifiable features in order to evade detection. Many of the common forms of malware can be polymorphic, including viruses, worms, bots, trojans, or keyloggers. Polymorphic techniques involve frequently changing identifiable characteristics like file names and types or encryption keys to make the malware unrecognizable to many detection techniques." Retrieved from https://digitalguardian.com/blog/what-polymorphic-malware-definition-and-best-practices-defending-against-polymorphic-malware

[37] FireEye, "Advanced Persistent Threat Groups" *op. cit.*

offensive or defensive in nature. Offensive operations are designed to support, through operations in cyberspace or targeting digital technologies, an objective of the terrorist group or nation-state to which the cyber unit belongs. Defensive operations are designed to prevent an adversary from carrying out digital surveillance or other forms of offensive operations. Ransomware was designed as a vehicle for obtaining money, usually in the form of a designated virtual currency such as bitcoin. In return for the payment, the victim received a key to decrypt the ransomware impacted files.

The discussion above demonstrated how ransomware can be used to obfuscate other operations, like data theft or unauthorized wire transfers. By its very nature, ransomware represents a powerful tool for carrying out actual offensive cyberwarfare against an enemy. Consider some recent cases in which cities like Rivera Beach and Lake City paid thousands of dollars in ransom. The cyber attackers spent enough time infiltrating the organizations' networks to enable file backup destruction before encrypting active files on both workstations and servers. Without hardened backups able to resist ransomware's operations, the cities were unable to manage basic needs. Furthermore, the cities of Atlanta and Baltimore spent millions of dollars in their attempts to rebuild the data which had been encrypted by successful ransomware attacks.

The fact is that when ransomware detonates without protected backups, organizations are incapacitated. Consider a hypothetical case: A civilian company is hired as a contractor to provide foodstuffs to support an in-country military operation. That company's operations are designed around an information system that takes orders a month in advance and arranges orders for fresh food – which may need to be shipped in from the homeland – so that deliveries can be made to military unit catering operations in a just-in-time supply process. The operation of the real-time system is key to getting the troops and support personnel in the field fed. Assume a terrorist group opposing the military force can get ransomware into the food contractor's system. They detonate it three days before a planned military operation. Suddenly, the contractor doesn't have access to what the company ordered from its vendors. It doesn't have access to the orders that it must prepare and send to military units. The military units involved could substitute ready-to-eat combat rations, but at what cost in time and aggravation? It could take significant time for the vendor to restore its operations – particularly if the terrorist group behind the attack had done surveillance and preparation and were able to encrypt the backup files. What if the attack targeted the military's logistics operation designed to provide ammunition? Or the systems used to coordinate with other military organizations? Or the aviation element's target selection system?

From the viewpoint of the victim organization, this appears to be a ransomware attack, with a request for a ransom payment. But the perpetrators have no intention of ever providing a decryption key. Indeed, it is to their advantage if the victim believes that paying the ransom will result in the delivery of a key. Payment can be used to finance the terrorist group's operations. The perpetrators could not send a key, or they could send a false key. In a more sophisticated attack, they could send a key that would only decrypt low-priority files, causing a delay in recovery efforts. The target of a terrorist group could also be a non-military or civilian site. Shutting down the 911 police dispatch system in a municipality, or the power system, or disabling an automatic teller machine network could serve the perpetrators by spreading the notion that people are not safe from terrorist attacks.

The authors propose that when malware, like ransomware, is re-purposed to cause damage in support of terrorist objectives, it should be referred to as "terrorware." The very concept of ransomware – denial of access to necessary files – is a natural attraction for terrorist groups. The technology to

carry out these attacks is, as was explained above, openly available for rent or purchase on the dark web.[38] Furthermore, when ransomware is re-purposed as terrorware, its use obfuscates its real motive – carrying out a terrorist cyber act. These same characteristics, of course, can also be used by a nation-state to carry out a cyber-offensive operation against a target. The availability of this malware should be a substantial motivator for potential victims to strengthen and maintain their cyberdefenses and assure that the structure of their systems provides for protected backup. If backup data is available, the effects of the attack can often be quickly mitigated. Unfortunately, too many organizations remain at risk.

Ransomware and the Difficulty of Malware Attribution

Malware attribution is the process of gathering evidence to determine who was behind any form of cyberattack. Attribution may be needed to support a criminal investigation or expose actions of a nation-state advanced persistent threat actor group. Malware technical analysis involves analyzing the attributes or behaviors of different pieces of the malware code, looking for markers that would allow an examiner to trace the evolution of the code, much like how a scientist might trace a species evolution through DNA mutations. There are numerous tools and resources such as *VirusTotal*, the FBI's *Malware Investigator* and *Joe Sandbox* that automate much of this process. Attribution is not, however, a perfect science. In the last half of 2018, the world was attacked with a particularly virulent strain of ransomware named Ryuk. Ryuk became famous (or perhaps infamous) when, on December 29, 2018 it spread across major U.S. publications, delaying or preventing the printing of *The Los Angeles Times*[39], *The San Diego Union-Tribune* and the west coast editions of *The Wall Street Journal* and *The New York Times.*[40]*"* The Ryuk "genetic signature" quickly showed the code had evolved from Hermes ransomware, which was the ransomware variant deployed by North Korean State Actors during their attack on the FEIB in Taiwan in October 2017. For several weeks, the media pointed to North Korea as the Ryuk threat actor. Weeks after the attack, however, several malware analysis teams began publishing results linking Ryuk to the sophisticated Russian cybercrime organization known as Grim Spyder[41]. It appears that the Grim Spyder group acquired the North Korean Hermes ransomware code either through outright purchase or as part of a Ransomware-as-a-Service type revenue-sharing agreement.

Ransomware-as-a-Service has made attribution much more difficult. Nation-state advanced persistent threat actor groups, cyber terrorists and sophisticated cybercrime organizations may have different underlying motives, but the lines are starting to blur as they work together to accomplish their collective goals and share the financial rewards.[42]

---

[38] The dark web refers to portions of the internet which are typically available only using specialized web browsers (like *The Onion Router*), and to which access is limited by those operating web sites on the dark web. This portion of the internet is often associated with criminal activity.

[39] Alpert Reyes, Emily, Barboza, Tony, & James, Meg. "Foreign cyberattack hits newspapers: Here is what we know." Retrieved December 29, 2018 at https://www.latimes.com/local/lanow/la-me-cyberattack-times-newspaper-malware-20181229-story.html

[40] Brewster, Thomas. "Mistaken for North Koreans, the 'Ryuk' Ransomware Hackers Are Making Millions." Retrieved February 20, 2019 at https://www.forbes.com/sites/thomasbrewster/2019/02/20/mistaken-for-north-koreans-the-ryuk-ransomware-hackers-are-making-millions/#2d2d7ecc75f4

[41] Hanel, Alexander. "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware." Retrieved January 10, 2019 at https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

[42] Schwartz, Mathew J. "Stop the Presses: Don't Rush Tribune Ransomware Attribution." Retrieved December 31, 2018 at https://www.bankinfosecurity.com/blogs/stop-presses-dont-rush-tribune-ransomware-attribution-p-2700

Conclusions and Recommendations for Action

Any analysis must start with the fact that ransomware is readily available for lease or purchase on the dark web and is a very effective t00ool used in cybercrime. It represents a way for criminal organizations, terrorist groups, and rogue nation-states to obtain substantial amounts of money which flows effortlessly through the underground cryptocurrency financial system. These cryptocurrencies can be used to evade sanctions and are easily used to buy other resources or converted into hard currencies. As far back as 2005, Islamic extremists were calling for the creation of an Islamist hackers' army to execute cyberattacks against the U.S. government. Postings on the extremism bulletin board *al-Farooq* included detailed cyberattack instructions and malware tools that could recover passwords of targeted users.[43] In a report to the U.S. Congress, the Congressional Research Service stated:

> "In April 2002, the Central Intelligence Agency (CIA) stated in a letter to the U.S. Senate Select Committee on Intelligence that cyber warfare attacks against the U.S. critical infrastructure will become a viable option for terrorists as they become more familiar with the technology required for the attacks. Also, according to the CIA, various groups, including Al Qaeda and Hizballah, are becoming more adept at using the Internet and computer technologies."[44]

The potential for combining a cyberattack with a kinetic attack is evident. Taking out a city's power supply before carrying out a terrorist attack would serve to magnify the impact of that event. Similarly, with services such as police communications, 911 emergency call operations and cell towers disabled, terrorists have a much higher chance of escape. There would also be a corresponding impact on the responsiveness of emergency workers, hospitals, and medical personnel as a cyberattack can quickly disable their ability to treat victims effectively.

Whether used as a tool to finance operations, a means to cover up an alternative cyber objective, or in support of a kinetic operation, ransomware is a real and effective tool of terror. The technical skill of the adversary, when combined with patient reconnaissance, greatly increases the breadth and effectiveness of an attack.

Can anything be done to prevent or reduce the effectiveness of cyberattacks? To the authors' knowledge, there is no perfect solution. Encryption algorithms used in professional ransomware are mathematically solid, and without a decryption key, the files they affect are unrecoverable. The large array of malware tools used as delivery vehicles are constantly evolving, matching the efforts of software developers and cybersecurity professionals to interdict or respond to them.

Organizations in both the public and private sectors should examine how they have structured their networks. Specific consideration should be given to virtual local area networks and internal firewalls that restrict lateral movement. Backup files should be stored such that they are isolated from the network and out of the reach of ransomware. Defeating terrorware starts with a discussion of ransomware's effectiveness as a weapon of destruction and working collectively on solutions with a focus on defense.

---

[43] Waterman, Shaun. "Islamists Seek to Organize Hackers' Jihad in Cyberspace." *Washington Times*, August 26, 2005, p. 9.

[44] Rollins, John, & Wilson, Clay. "Terrorist Capabilities for Cyberattack: Overview and Policy Issues." *Congressional Research Service Report for Congress RL33123*, January 22, 2007.

The authors' objective is to brief the anti-terrorist and cyberwarfare communities on the potential use of ransomware for funding terrorist or rogue states, for obfuscating other intrusions into their systems, and of the use of ransomware in the form of terrorware, intended to damage the ability of targeted organizations to operate. We hope that it will help potential victims understand the risks and the ways that this form of malware can be used and provide recommendations for mitigating the risks faced with the evolution and use of ransomware by cyber-criminals, terrorist groups and nation-states alike.

References

Ackerman, Devon. "Evolving World of Cybercrime – Banking Trojans and Ransomware Deployment" Kroll Insights, May 19, 2019. Accessed October 11, 2019 at https://www.kroll.com/en/insights/publications/cyber/cybercrime-banking-trojans-ransomware

Brewster, Thomas. "Mistaken for North Koreans, the 'Ryuk' Ransomware Hackers Are Making Millions." Forbes.com, February 20, 2019. Accessed October 10, 2019 at https://www.forbes.com/sites/thomasbrewster/2019/02/20/mistaken-for-north-koreans-the-ryuk-ransomware-hackers-are-making-millions/#2d2d7ecc75f4

Brill, Alan, & Keene, Lonnie. "Cryptocurrencies: The Next Generation of Terrorist Financing?" *Defense Against Terrorism Review, 6*(1), Spring & Fall 2014.

Brill, Alan, & Smolanoff, Jason. "Hacking Back Against Cyberterrorists: Could you? Should you?" *Defense Against Terrorism Review, 9*, 2017

Cimpanu, Catalin. "North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist." BleepingComputer.com, October 17, 2017. Accessed October 9, 2019 at https://www.bleepingcomputer.com/news/security/north-korean-hackers-used-hermes-ransomware-to-hide-recent-bank-heist/

Council on Foreign Relations, *CyberOperations Tracker*, "APT 37." n.d. Accessed October 10, 2019 at https://www.cfr.org/interactive/cyber-operations/apt-37

Department of the Treasury (U.S.) "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups." September 13, 2019. Accessed October 11, 2019 at https://home.treasury.gov/index.php/news/press-releases/sm774

Dudley, Renee. "The Extortion Economy: How Insurance Companies are Fueling a Rise in Ransomware Attacks." *ProPublica*, August 27, 2019. Accessed Oct 8, 2019 at https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

Dudley, Renee, & Kao, Jeff. "The Trade Secret: Firms that Promised High=Tech Ransomware Solutions Almost Always Just Pay the Hackers." *ProPublica*, May 15, 2019. Accessed October 8, 2019, at https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

Entenmann, Eva, & van den Berg, Willem. "Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?" November 1, 2018. Accessed October 8, 2019 at https://icct.nl/publication/terrorist-financing-and-virtual-currencies-different-sides-of-the-same-bitcoin/

Federal Bureau of Investigation (U.S.). "Ransomware Suspects Indicted: Iranian Man Charged with Deploying Damaging *SamSam* Ransomware." November 18, 2018. Accessed October 8, 2019 at https://www.fbi.gov/news/stories/iranian-ransomware-suspects-indicted-112818

Fernandez, Manny, Sanger, David E., & Martinez, Marina Trahan. "Ransomware Attacks are Testing the Resolve of Cities Across America.". *The New York Times*, August 22, 2019.

Fireeye. "Advanced Persistent Threat Groups." n.d. Accessed October 11, 2019 at https://www.fireeye.com/current-threats/apt-groups.html

Ford, Wayne. "Cyber attack forces Jackson County to pay $400,000 ransom." *The Athens [Georgia] Banner Herald*, March 8, 2019.

Fruhlinger, Josh. "Marriott data breach FAQ: How did it happen and what was the impact?" *CSO Online*, September 30, 2019. Accessed October 10, 2019 at https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html .

Hanel, Alexander. "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware," January 10, 2019. Accessed October 10, 2019 at https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Kass, D. H. "Riviera Beach Florida Ransomware Attack: City Pays $600,000." Retrieved October 8, 2019 at https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/riviera-beach-florida-malware-attack/

Kujawa, Adam. "Under the Radar – The Future of Undetected Malware," Malwarebytes. Accessed October 10, 2019 at https://resources.malwarebytes.com/resource/under-the-radar-the-future-of-undetected-malware/?utm_source=blog&utm_medium=post&utm_campaign=q4fy19

Liska, Allan. "Early Findings: Review of State and Local Government Ransomware Attacks." *Recorded Futures*, May 10, 2019. Accessed October 11, 2019 at https://www.recordedfuture.com/state-local-government-ransomware-attacks/

Nichols, Michelle. "North Korea generated $2B from cybercrime to fund nuclear weapons program: U.N. report." *Reuters*, August 5, 2019. Accessed October 8, 2019 at https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

Palo Alto Networks. "How to Break the Cyber Attack Lifecycle," n.d. Accessed October 10, 2019 at https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

Reyes, Emily Alpert, Barboza, Tony, & James, Meg. "Foreign cyberattack hits newspapers: Here is what we know", *Los Angeles Times*, December 29, 2018.

Rollins, John, & Wilson, Clay. "Terrorist Capabilities for Cyberattack: Overview and Policy Issues" *Congressional Research Service Report for Congress RL33123*, January 22, 2007.

Schwartz, Mathew J. "Stop the Presses: Don't Rush Tribune Ransomware Attribution", BankInfoSecurity.com, December 31, 2018. Accessed October 11, 2019 at https://www.bankinfosecurity.com/blogs/stop-presses-dont-rush-tribune-ransomware-attribution-p-2700

Sette, Nichole, & Hanson, Scott, "Ransomware on the Rise," *Kroll's the Monitor*, Issue 8. October 7, 2019. Accessed October 8, 2019 at https://www.kroll.com/en/insights/publications/cyber/monitor/ransomware-rise-monitor-issue

Waterman, Shaun. "Islamists Seek to Organize Hackers' Jihad in Cyberspace." *The Washington Times*, August 26, 2005.

Yan, S. "US report says APT38 behind Taiwanese bank NT$1.8 billion cyberheist." *Taiwan News*. Accessed October 04, 2018 at https://www.taiwannews.com.tw/en/news/3544541

DATR, 2019; 12 : 59-83

ISSN 1307 - 9190

Assessing Legal and Policy Responses to Boko Haram's Terrorism in Nigeria

Dr. Uchenna Jerome Orji [1]
Asst. Professor, School of Law, American University of Nigeria, Yola, Nigeria

Abstract: *Since 2009, Nigeria has been challenged by the terrorist activities of the Boko Haram Islamist sect in the north-eastern part of the country. The sect is opposed to the spread of western values and education, which it perceives as threatening traditional values, beliefs, and customs among Muslim communities in northern Nigeria. In order to propagate its extremist religious ideology, Boko Haram has carried out several mass casualty attacks that include the use of armed gunmen, Improvised Explosive Devices (IEDs) and suicide bombings. By 2019, the sect was estimated to have killed over 37,500 people and destroyed properties worth over $5.2 billion, while also causing the forceful displacement of over 2.5 million people from their homes. In order to tackle the violent acts of Boko Haram, the Nigerian government has established legal and policy counter terrorism measures. For example, in 2011, Nigeria enacted the Terrorism (Prevention) Act (which was later amended in 2013). This is in addition to several policy instruments that are meant to counter terrorist activities such as the National Counter Terrorism Strategy, the Nigerian National Security Strategy, and the National Action Plan for Preventing and Countering Violent Extremism. However, the question arises as to whether the establishment of legal and policy measures for countering terrorist activities has effectively contributed in tackling the violent extremist activities of the Boko Haram sect? This paper will examine the efficacy of Nigeria's counter terrorism laws and policies in tackling the terrorist activities of Boko Haram. In so doing, the paper indentifies factors that have impeded the effective enforcement of Nigeria's counter terrorism measures in tackling Boko Haram's activities and further propose responses that can be adopted to improve their enforcement and implementation.*

Keywords: *Nigeria; Religious extremism; Boko Haram; Counter terrorism law and policy.*

[1] LL.B (Hons.), (University of Nigeria); LL.M (University of Ibadan); PhD (Nnamdi Azikiwe University Nigeria); Barrister and Solicitor of the Supreme Court of Nigeria. Email: This paper is a modified version of a paper titled: "Tackling the Violent Religious Extremism of Boko Haram: An Inquiry into the Efficiency of Nigeria's Counter Terrorism Regime", presented at the International Conference on Religious Violence and Extremism at Bar IIan University, Ramat Gan, Israel (28-30 May, 2018) with the support of the Faculty of Law, Bar IIan University. The author is solely responsible for the views expressed in this paper, and neither does the paper represent the views of any national or international organization(s) that the author consults for, or has consulted for or, is affiliated to.

Introduction

For about a decade, Nigeria has been challenged by the terrorist activities of Boko Haram. Boko Haram is also known as *Jama'atul Alhul Sunnah Lidda'wati wal Jihad*, which means "people committed to the propagation of the Prophet's teachings and jihad".[2] The sect is opposed to the spread of western values and education, which it perceives to be a threat to the religious values and beliefs of Muslim communities in northern Nigeria, and the group instead advocates the practice of a very strict and harsh form of Islamic law (Sharia law) amongst Muslims.[3] It does not recognize the authority of the Nigerian State and it also encourages Muslims to engage in active Jihad in order to spread the Islamic faith and defend the global community of Muslims.[4] Major objectives of the sect include establishing an Islamic Caliphate in Nigeria[5] and Islamizing the Nigerian State.[6] The sect does not tolerate disagreement with its extremist religious ideology and deploys violence as a tool for spreading its message. Since 2009, Boko Haram has carried out several deadly mass casualty attacks that include the use of armed gunmen, Improvised Explosive Devices (IEDs), and suicide bombers.[7] By 2019, the group was estimated to have killed over 37,500 people and causing the forceful displacement of over 2.5 million people from their homes.[8] In Borno State (one of the States affected by the terrorist activities of Boko Haram), it is estimated that the sect destroyed properties worth over $5.2 billion.[9]

In order to tackle terrorism, the government of Nigeria has established a range of legal and policy measures instruments, including the Terrorism (Prevention) Act,[10] the Economic and Financial Crimes Commission (Establishment) Act,[11] the Money Laundering (Prohibition) Act,[12] the National Counter Terrorism Strategy,[13] the Nigerian National Security Strategy,[14] and the National Action Plan for Preventing and Countering Violent Extremism.[15] However, the question arises as to whether the establishment of legal and policy measures for countering terrorism has effectively contributed to tackling the terrorist activities of Boko Haram. In order to address this question, this paper adopts as a doctrinal research method to undertake an analytical review of Nigeria's counter terrorism laws and policies. The paper refers to the Nigerian Constitution and Nigeria's counter terrorism laws and

---

2 *See* James J.F. Forest, *Confronting the Terrorism of Boko Haram in Nigeria* (Joint Special Operations University Press, Florida, United States, 2012) p.62. *See also*, Farourk Chothia, 'Who are Nigeria's Boko Haram?', *BBC News* (26 August, 2011), available at <http://www.bbc.co.uk/new/world-africa-13809501> last accessed on 16 January 2020.

3 *See* James J.F. Forest, *ibid*, p.1.

4 *See* Andrew Walker, 'What is Boko Haram?', *United States Institute of Peace Special Report* (June, 2012) pp. 1-6.

5 *See* Tolulope Ola-David, 'Is Boko Haram re-creating a Caliphate in Africa?', *Global Risks Insights* (4 September, 2015), available at <https//www.globalriskinsights.com/2015/09/is-boko-haram-re-creating-a-caliphate-in-africa/>last accessed on 16 January 2020.

6 *See* James Adewunmi Falode, 'The Nature of Nigeria's Boko Haram War, 2010-2015: A Strategic Analysis', *Perspectives on Terrorism* (2016) Vol.10 (1), pp.47.

7 *See* Counter Extremism Project, *Boko Haram* (2019), pp.1-53, available at <https://www.counterextremism.com/threat/boko-haram> last accessed on 16 January 2020.

8 *See* Council on Foreign Relations, *Global Conflict Tracker: Boko Haram in Nigeria* (31 October, 2019), available at <https://www.cfr.org/interactive/global-conflict-tracker/conflict/boko-haram-nigeria> last accessed on 16 January 2020.

9 *See* Conor Gaffey, 'Cost of Terrorism: Boko-Haram has Destroyed $5.2 Billion Worth of Property in just One State in Nigeria', *Newsweek* (8 August, 2017) available at <http://www.newsweek.com/cost-terrorism-boko-haram-nigeria-64854>.

10 *See* Terrorism (Prevention) Act, No.10 (2011). *See* Terrorism (Prevention) (Amendment) Act (2013).

11 *See* Economic and Financial Crimes Commission (Establishment) Act 2004.

12 *See* Money Laundering Prohibition Act 2011.

13 *See* Office of the National Security Adviser, *The National Counter Terrorism Strategy (Revised)* (2016).

14 *See* Federal Republic of Nigeria, *National Security Strategy* (November, 2014).

15 *See* Federal Republic of Nigeria, *Policy Framework and National Action Plan for Preventing and Countering Violent Extremism* (August, 2017).

policies, as well as information in books, journals, magazines and other published studies relating to Boko Haram and counter terrorism in Nigeria. The paper identifies factors impeding the enforcement of Nigeria's counter terrorism measures in tackling the activities of Boko Haram, including the inefficient investigation and prosecution of cases, weak synergy between security forces and law enforcement institutions, challenges related to the tracking and freezing of the group's finances, and inadequate responses towards addressing the root causes of violent extremism. The paper also proposes measures to improve the implementation and enforcement of Nigeria's counter terrorism measures. The paper recommends a review of the detention powers under section 27(3) of the Terrorism Prevention (Amendment) Act and the establishment of a justice administration policy that will facilitate the expeditious prosecution of cases involving members of Boko Haram.

This paper consists of five sections with this introduction being the first. The second section discusses the emergence of Boko Haram and its particular brand of violent extremism. The third section reviews Nigeria's counter terrorism measures. The fourth section discusses the implementation of Nigeria's counter terrorism measures and identifies factors that have impeded effective enforcement while also proposing responses that can be adopted to improve its enforcement and implementation, followed by conclusions.

2. The Boko Haram Islamist Sect and its Violent Extremism

There are several accounts of the origins of Boko Haram. One account states that Boko Haram emerged in the mid-1990's, led by Abubakar Lawan and later by Aminu Tashen-Ilimi.[16] Another account states that Boko Haram emerged from a radical Islamist youth group that worshipped at the Alhaji Muhammadu Ndimi Mosque in Maiduguri, Borno State, around 2002, which was led by a charismatic young Muslim cleric known as Mohammed Yusuf.[17] An account by the Nigerian Government indicates that the sect first emerged in Borno State in 2000.[18] Yet another account which has been referenced in a Nigerian Government White Paper states that Boko Haram evolved from private militias set up by some prominent politicians in States in the north-eastern part of Nigeria to outflank political opponents ahead of the 2003 general elections.[19] After the elections, the private militias, which mostly comprised unemployed youths, were discarded by their sponsors and later became easy prey for the radical brand of Islam preached at that time Boko Haram.[20]

By the beginning of 2009, the activities of Boko Haram had started to attract the attention of government authorities.[21] Boko Haram began fighting the government on 26 July, 2009, in Bauchi, Bauchi State, after the Police arrested several suspected leaders of the sect Boko Haram and in response its members attacked and destroyed a police station in Bauchi. In a short time, the violence spread to

---

[16] *See* Foard Copeland, *The Boko Haram Insurgency in Nigeria* (The Civil – Military Fusion Centre, February, 2013) p.1.

[17] *See* Andrew Walker, 'What is Boko Haram?', *United States Institute of Peace Special Report* (June, 2012) p.3. *See* Stephen Buchana – Clarke and Peter Knoope, 'The Boko Haram Insurgency: From Short Term Gains to Long Term Solutions', *Institute for Justice and Reconciliation Occasional Paper* (January, 2017) No.23 p.7.

[18] *See* Nigeria National Counter Terrorism Strategy (Office of the National Security Adviser, Abuja, August, 2016) p.7 at paragraph 3.

[19] *See* Ini Ekott, 'Government White Paper Indicts Prominent Politicians for Creating Boko Haram', *Premium Times* (28 April, 2013), available at <https://www.premiumtimes.ng.com/news/131/694-government-white-paper-indicts-prominent-politicians-for-creating-boko-haram.htm> last accessed on 16 January 2020.

[20] *Ibid*.

[21] *See* Freedom C. Onuoha, 'The Islamist Challenge: Nigeria's Boko Haram Crisis Explained', *African Security Review* (June, 2010) Vol. 19(2), p.58.

three other States including Borno, Yobe, and Kano.[22] The Nigerian government responded by deploying the Nigerian Army to assist the police in tackling the spreading violence, by the time the violence was contained, over 800 people were reported to have died.[23] Mohammed Yusuf, along with his father in-law and many members of the sect were arrested and paraded outside police stations. However, after spending a few hours in police custody, Mohammed Yusuf was extra judicially executed. The Army insisted that he was handed to over to the Police alive, while the Police claimed that he was shot while trying to escape.[24] The Police claimed that other members of the sect they were killed during an intense gun battle.[25] However, videos showing that the Police carried out a coldblooded extra-judicial execution of many captured Boko Haram members and their sympathizers later went viral on YouTube and other social media platforms.[26] The Government of Nigeria set up a Panel of Inquiry to probe the circumstances that led to the killing of Mohammed Yusuf.[27] In 2011, the government brought criminal proceedings against four policemen for allegedly killing Mohammed Yusuf.[28] However, those police officers were later acquitted by the Court in 2015 and reinstated into the Nigerian Police in 2018.[29]

The killing of Mohammed Yusuf and several captured Boko Haram members in July, 2009, is regarded as a turning point in the transformation of Boko Haram into a violent Islamist sect.[30] Thus, the brutal suppression of the 2009 Boko Haram uprising by the Nigerian government as well as the circumstances surrounding the extra-judicial killing of Mohammed Yusuf fueled local resentment and amplified "pre-existing animosities" towards the Nigerian government,[31]and further swelled Boko Haram's ranks with new members and sympathizers.[32] This state of affairs, coupled with increasing poverty, deteriorating social services and infrastructure, educational backwardness, massive youth unemployment, rising population of unemployed graduates, dwindling profits from agriculture and the weak productive base of the economy of northern Nigeria created a favorable environment for the rise of Boko Haram.[33] Also, the increasing accumulation of religious and socio-economic and political grievances, which Boko Haram had sought to address by establishing a perfect Islamic society apparently made the adoption of a terrorist campaign an attractive and justifiable option to the sect.[34]

---

22 *Ibid*, pp.58-60.

23 *See* James J.F. Forest, *Confronting the Terrorism of Boko Haram in Nigeria* (Joint Special Operations University Press, Florida, United States, 2012) p.64.

24 *See* Freedom C. Onuoha, *See* Freedom C. Onuoha, The Islamist Challenge: Nigeria's Boko Haram Crisis Explained', *African Security Review* (June, 2010) Vol. 19(2), p.60.

25 *See* James J.F. Forest, *ibid*.

26 *See* Aljazeera, 'Nigeria Killings Caught on Video', (10 February, 2010), available at <https://www.aljazeera.com/news/africa/2010/02/20102505798741.html> last accessed on 16 January 2020.

27 *See* Human Rights Watch, 'Nigeria: Prosecute Killings by Security Forces', (26 November, 2009/11/26/Nigeria-prosecute-killings-security-forces>last accessed on 16 January 2020.

28 *See* BBC, 'Nigeria Policemen in Court Trial for Boko Haram Killing', *BBC News* (13 July, 2011) available at <http://www.bbc.com/news/world-africa-14136185> last accessed on 16 January 2020.

29 *See* AFP, 'Policemen Accused of Killing Boko Haram Founder Reinstated', *The Guardian* (19 February, 2018) available at <https://m.guardian.ng/news/policemen-accused-of-killing-boko-haram-founder-reinstated/>. *See also* Roland Mutum and John Chuks Azu, 'Police Reinstate Officers Acquitted of Killing Boko Haram Leader', *Daily Trust* (19 February, 2018) available at <https://www.dailytrust.com.ng/police-reinstate-officers-acquitted-of-killing-Boko-haram-leader.html> last accessed on 16 January 2020.

30 *See* James J.F. Forest, *Confronting the Terrorism of Boko Haram in Nigeria* (Joint Special Operations University Press, Florida, United States, 2012) p.64.

31 *See* James J.F. Forest, *ibid* at p.64.

32 *See* Foard Copeland, *The Boko Haram Insurgency in Nigeria* (The Civil – Military Fusion Centre, February, 2013) p.3.

33 *See* Isa Muhammad, 'Militant Islamist Group, in Northern Nigeria', in Wafula Okumu and Augustine Ikelegbe (eds) *Militias, Rebels and Islamic Militants: Human Insecurity and State Crises in Africa* (Institute for Security Studies: Pretoria) p.329.

34 *See* James J.F. Forest, *ibid* at p.65.

In mid-2010, Boko Haram returned to Maiduguri under the leadership of Abubakar Shekau and unleashed a campaign of terror that included targeted assassinations and "hit and run" attacks against the Police in Borno and Yobe States.[35] The Sect also began to assassinate local leaders and other individuals who had cooperated with the Police and Army during the suppression of the 2009 Boko Haram uprising.[36] In its campaign of violence, Boko Haram deployed tactics such as the use of armed gunmen, suicide bombers, and IEDs.[37] The group also began to rob banks, cash-in-transit convoys and businesses;[38] and organized several successful prison breaks to free its members held in prison custody.[39] Another dimension to its campaign of terror was the kidnapping of women and school girls, notably the kidnapping of 276 girls from a secondary school in Chibok, Borno State, in April 2014, which attracted much global attention and condemnation, and leading to the "Bring Back Our Girls" movement.[40]

By 2014, Boko Haram also began to seize towns and villages in parts of north-eastern Nigeria, declaring them part of an Islamic Caliphate.[41] Prior to this, the Nigerian government had formally issued a Proscription Order which banned Boko Haram as a terrorist organization under section 2 of the Terrorist (Prevention) Act of 2011.[42] The government's proscription of Boko Haram as a terrorist organization was severely criticized by prominent social-political groups in northern Nigeria who felt that the move scuttled efforts to negotiate an end to the sect's terrorist activities by granting amnesty to members of the sect.[43] However, prior to the proscription, the government had set up a panel to examine the possibility of granting amnesty to members of Boko Haram. The idea of amnesty was however rejected by the group as they argued that they had done nothing wrong, and that it was the government who had committed atrocities against Muslims.[44] The United States Department of State also designated Boko Haram as foreign terrorist organization in November, 2013,[45] while the United Nations Security Council added the sect to its list of entities subject to targeted financial sanctions and arms embargo May, 2014.[46]

---

35 *See* Andrew Walker, 'What is Boko Haram?', *United States Institute of Peace Special Report* (June, 2012), p.5.

36 *Ibid*.

37 *Ibid*.

38 *See* Ali Adoji, 'Boko Haram Robs Bank, Kills 4 in Maiduguri', *Daily Post* (31 March, 2012) available at <http://dailypost.ng/2012/03/31/boko-haram-robs-bank-kills-4-in-maiduguri/> last accessed on 16 January 2020.

39 *See* David Smith, 'More than 700 Inmates Escape during Attack on Nigerian Prison', *The Guardian* (8 September, 2010) available at <https://www.theguardian.com/world/2010/Sep/08/muslim-extremists-escape-nigeria-prison>;Reuters, 'Gunmen Free 175 Inmates in Nigeria Prison Break', *The Telegraph* (30 June, 2013) available at <https://www.telegraph.co.uk/news/worldnews/africaandindianocean/nigeria/1015154.6/ Gunmen-free-175-inmates-in-Nigeria-prison- break.html> last accessed on 16 January 2020.

40 *See* Jacob, Zenn, 'Boko Haram and the Kidnapping of the Chibok School Girls', *CTC Sentinel* (May, 2014) Vol.7 (5) pp. 1-7.

41 *See* BBC 'Boko Haram Declares 'Islamic State' in Northern Nigeria', *BBC News* (25 August, 2014), available at <http://www.bbc.com/news/world-africa-28925484> last accessed on 16 January 2020.

42 *See* Terrorism (Prevention) (Proscription Order) Notice, 2013, *Official Gazette of the Federal Republic of Nigeria*, (24 May, 2013) Vol. 100, No. 34, pp. B53-55.

43 *See* Tobi Adeyeye, 'Northern Groups Protest Ban on Boko Haram, Ansaru', *The Herald* (6 June, 2013) available at <http://www.hearld.ng/northern-groups-protest-ban-on-boko-haram-ansaru/>;Ameh Comrade Godwin, 'North Kicks against FG's Decision to Ban Boko Haram, Ansaru', *Daily Post* (6 June, 2013), available at <http://dailypost.ng/2013/06/06/north-kicks-against-fgs-decision-to-ban-boko-haram-ansaru/> last accessed on 16 January 2020.

44 *See* BBC, 'Nigeria's Boko Haram Rejects Jonathan's Amnesty Idea', *BBC News* (11 April, 2013) available at <http://www.bbc.com/news/world-africa-22105476> last accessed on 16 January 2020.

45 *See* United States Department of State, 'Foreign Terrorist Organizations', available at <https://www.state.gov/j/ct/rls/other/des/123085.htm>;Counter Terrorism Guide, 'Boko Haram', available at <https://www.dni.gov/nctc/groups/boko_haram.html> last accessed on 16 January 2020.

46 *See* United Nations, 'Sanctions Committee Adds Boko Haram to its Sanctions List', *United Nations Press Release* (22 May, 2014) SC/11410, available at <https://www.un.org/press/en/2014/sc11410_do.htm> last accessed on 16 January 2020.

Despite the proscription of Boko Haram and the government's declaration of a state of emergency to enable the military to tackle the group's terror campaign and its incursion into towns and villages in north-eastern Nigeria, the government did not record significant military success against Boko Haram due to several factors. These included: a lack of modern military equipment; poor training; low motivation amongst fighting troops; the deployment of brutal military tactics, resulting in collateral damage and a loss of trust amongst the civilian population; poor human rights record of military authorities; poor funding of the military; and corruption.[47] Although statements from the Nigerian government between the end of 2015 and 2019 claimed that Boko Haram have been "technically" or "completely" defeated by the military,[48] some reports have contradicted such claims.[49] For example, the sect is reported to have killed over 1,100 persons and carried out over 181 attacks between 2016 and 2017, despite being declared "technically defeated".[50] A recent report also observes that "Boko Haram militants now control four zones in northern Borno State, near Lake Chad. They are well-armed following raids on military facilities, and now employ the use of sophisticated drones. The military is increasingly on the defensive, holding up in heavily fortified super camps".[51]

This state of affairs clearly indicates that the sect is still active and violent although its activities may have been largely curtailed by on-going military and security operations in the north-eastern region of Nigeria. A full military defeat of Boko Haram will not, however, eradicate the sect's extremist religious ideology where the elements that contributed to the emergence of the sect (such as widespread poverty, inequality, unemployment, accumulated social economic and political grievances and high handedness by government security forces) still persist.[52]

3. An Overview of Nigeria's Counter Terrorism Regime

47 *See* Andrew Walker, 'Why Nigeria has not Defeated Boko Haram', *BBC News* (14 May, 2014) available at <https://www.bbc.com/news/world-africa-27396702> last accessed on 16 January 2020; Habibu Yaya Bappah, 'Nigeria's Military Failure against the Boko Haram Insurgency', *African Security Review* (2016) Vol. 25(8) pp. 1-13.

48 *See* Christopher Giles, 'Nigerian Elections: Has Boko Haram Been Defeated?', *BBC News* (8 February, 2019), available at <https://www.bbc.com/news/world-africa-47047399>; BBC, 'Nigeria Boko Haram Militants Technically Defeated – Buhari', *BBC News* (24 December, 2015) available at <https://www.bbc.com/news/world-africa-35173618>; Ndahi Marama, 'Boko Insurgents Have Been Defeated – Buratai', *Vanguard* (8 January, 2018), available at <https://www.vanguard.ngr.com/2018/01/boko-haram-insurgents-defeated-buratai>; Seun Opejobi, 'Buhari Claims Boko Haram Technically Defeated', *Daily Post* (6 February, 2016) available at <http://dailypost.ng/2016/02/06/buhari-claims-boko-haram-technically-defeated/> last accessed on 16 January 2020.

49 *See* John Campbell, 'Boko Haram is Back in the Media Spotlight, but it was Never Really Gone', *Council on Foreign Relations* (20 September, 2019), available at <https://www.cfr.org/blog/boko-haram-back-mdeias-spotlight-it-was-never-really-gone>; Abdulkareem Haruna , 'Why Nigerian Army has not defeated Boko Haram- Theatre Commander', Premium Times (11 October, 2019), available at <https://www.premiumtimesng.com/news/headlines/357102-why-nigerian-army-has-not-defeated-boko-haram-theatre-commander.html>; Dionne Searcey, 'Boko Haram is Back with Better Drones', The New York Times (13 September, 2019), available at <https://www.nytimes.com/2019/09/13/world/africa/nigeria-boko-haram.html> last accessed on 16 January 2020.

50 *See* Abubakar Adam Ibrahim, 'Boko Kills 1,100 Since Being Technically Defeated', *Daily Trust*, (3 December, 2017), available at <https://www.dailytrustcom.ng/boko-haram-kills-1-100-since-being-technically-defeated-html>; Shakirudeen Taiwo, 'Technically Defeated Boko Haram Carried out 135 Terror Attacks in 2017 – UN Envoy", *Business Insider* (12 January, 2018), available at <http://www.pulse.ng/bi/politics/technically-defeated-boko-haram-carried-out-135-attacks-id7837805.html> last accessed on 16 January 2020.

51 *See* John Campbell, 'Boko Haram is Back in the Media Spotlight, but it was Never Really Gone', *Council on Foreign Relations* (20 September, 2019).

52 *See* David Doukhan, *Defeating Boko Haram: The Realty on the Ground is Deceptive* (International Institute for Counter Terrorism: Israel, 26 November, 2015) pp.1-26.

Nigeria has established several legal and policy instruments that are meant to curb terrorist activities. Such legal and policy instruments include the Terrorism (Prevention) Act,[53] the Economic and Financial Crimes Commission (Establishment) Act,[54] the Money Laundering (Prohibition) Act,[55] the National Security Strategy,[56] the National Counter Terrorism Strategy,[57] and the Policy Framework and National Action Plan for Promoting and Countering Violent Extremism.[58] This section will review these legal and policy instruments.

3.1 The Terrorism (Prevention) Act

The Terrorism (Prevention) Act was originally enacted in 2011.[59] Prior to that time, attempts by the Nigerian government to establish a comprehensive counter terrorism law suffered setbacks due to the government's lack of political will and concerns that such law could be exploited by the government to muffle political opponents and critics.[60] The blacklisting of Nigeria by the United States as a "Country of Interest" on its Terror Watch List following an unsuccessful attempt by a Nigerian, Umar Farouk Abdulmutallab, to detonate an explosive on board a United States-bound North West Airlines flight on 25 December, 2009, however, necessitated the need to establish a counter terrorism policy.[61] One of the conditions the United States gave to delist Nigeria from its Terror Watch List was the enactment of a counter terrorism law in the country.[62] In response, the Terrorism (Prevention) Act was enacted in June, 2011. The Act is regarded as "a veritable watershed in law making in Nigeria" due to its comprehensive scope.[63] In 2013, the Act was amended to further expand the scope of offences and also improve inter-agency cooperation on counter-terrorism.[64]

The Terrorism (Prevention) Act prohibits all "acts of terrorism" and "terrorism financing".[65] The Act does not explicitly define the meaning of 'terrorism", although it broadly defines "an act of terrorism" under section 1(2) as "an act which is deliberately done with malice, after thought and which:

(a) may seriously harm or damage a country or an international organization;

(b) is intended or can reasonably be regarded as having been intended to -

(i) unduly compel a government or international organization to perform or abstain from performing any act;

---

53 *See* Terrorism (Prevention) Act, No.10 (2011). *See* Terrorism (Prevention) (Amendment) Act 2013, *Official Gazette of the Federal Republic of Nigeria* (22 April, 2013) Vol. 100, No.25, Government Notice, 70, pp. A27-A52.

54 *See* Economic and Financial Crimes Commission (Establishment) Act 2004.

55 *See* Money Laundering Prohibition Act 2011.

56 *See* Federal Republic of Nigeria, *National Security Strategy* (November, 2014).

57 *See* Office of the National Security Adviser, *The National Counter Terrorism Strategy (Revised)* (2016).

58 *See* Federal Republic of Nigeria, *Policy Framework and National Action Plan for Preventing and Countering Violent Extremism* (August, 2017).

59 *See* Terrorism (Prevention) Act, No.10 (2011).

60 *See* Isaac T. Sampson and Freedom C. Onuoha, 'Forcing the Horse to Drink or Making it Realize its Thirst? : Understanding the Enactment of Anti-Terrorism Legislation (ATL) in Nigeria', *Perspectives on Terrorism* (2011) Vol. 5(3-4), p.39.

61 *Ibid*, pp.40-41.

62 *See* Sufuyan Ojeifo, and Onwuka Nzechi, 'Terror Blacklist: US Gives Nigeria Four Conditions', *Thisday* (12 February, 2010), available at <http://www.thisdayonline.com/nview.php?id= 166347> last accessed on 16 January 2020.

63 *See* Akin Oyebode, 'Legal Responses to the Boko Haram Challenge: An Assessment of Nigeria's Terrorism (Prevention) Act 2011', *Forum on Public Policy* (2012) p.12.

64 *See* Terrorism (Prevention) (Amendment) Act 2013, *Official Gazette of the Federal Republic of Nigeria* (22 April, 2013) Vol. 100, No.25, Government Notice, 70, pp. A27-A52.

65 *See* Section 2(a) (1) Terrorism (Prevention) (Amendment) Act, 2013.

(ii) *seriously intimidate a population*;

(iii) seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country, or an international organization; or,

(iv) otherwise influence such government or international organization by intimidation or coercion; and,

(c) involves or causes as the case may be -

(i) an attack upon a person's life which may cause serious bodily harm or death;

(ii) kidnapping of a person;

(iii) destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss;

(iv) the seizure of an aircraft, ship or other means of public or goods transport and diversion or the use of such means of transportation for any of the purpose in paragraph (b) (ix) of this subsection;

(v) the manufacture, possession, acquisition, transport, apply or use of weapons, explosives, or nuclear, biological or chemical weapons, as well as research into, and development of biological and chemical weapons without lawful authority;

(vi) the release of dangerous substance or causing of fire, explosions or floods, the effect of which is to endanger human life;

(vii) interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;

(d) An act or omission in or outside Nigeria which constitutes an offence within the scope of counter terrorism protocols and conventions duly ratified by Nigeria".[66]

This definition of acts of terrorism broadly criminalizes violent extremist acts such as those carried out by Boko Haram. This is because the sect aims to Islamize the Nigerian State through the propagation its religious beliefs and uses violent acts that are explicitly classified as acts of terrorism to achieve that objective. In addition to the acts of terrorism classified under section 1(2) of the Terrorism (Prevention) Act, an act of protest which disrupts a service is classified as an act of terrorism where such act of protest is intended to unduly compel a government or international organization to perform or abstain from performing any act, or where such an act of protest is intended to seriously intimidate a population.[67] However, a demonstration such as a labour strike or stoppage of work is not considered to constitute an "act of terrorism" where such an act is not intended to unduly compel a government or international organization to perform or abstain from any act.[68]

The Terrorism (Prevention) Act provides for the proscription of organizations that are established to promote or incite acts of terrorism.[69] For example, Boko Haram was proscribed in 2013.[70] Acts

---

66 *See* Section 1(2) Terrorism (Prevention) Act 2011 (Emphasis added).

67 *See* Section 1 (3) Terrorism (Prevention) Act 2011.

68 *See* Section 1 (3) Terrorism (Prevention) Act 2011.

69 *See* Section 2 Terrorism (Prevention Act) 2011.

70 *See* Terrorism (Prevention) (Proscription Order) Notice, 2013, *Official Gazette of the Federal Republic of Nigeria*, (24 May, 2013) Vol. 100, No. 34, pp. B53-55.

that are specifically prohibited under the Terrorism (Prevention) Act include: arranging, or assisting, or participating in a meeting connected with an act of terrorism or a terrorist group;[71] soliciting or rendering support to a terrorist group for the purposes of committing acts of terrorism;[72] harboring a terrorist or hindering the arrest of a terrorist;[73] providing training or instruction to terrorists or terrorist groups;[74] concealing relevant information that will assist in preventing the commission of an act of terrorism or securing the apprehension, prevention or conviction of a person for an act of terrorism;[75] providing or offering to provide an explosive device or any other lethal device to a terrorist or terrorist group;[76] recruiting persons to carry out terrorist acts or to become members of a terrorist group;[77] inciting the commission of a terrorist act, promoting the membership of a terrorist group, soliciting property for the benefit of a terrorist group or for the commission of terrorist act;[78] providing facilities to support the commission of terrorist acts;[79] terrorist financing;[80] dealing in terrorist funds or property;[81] hostage taking;[82] professing membership of a terrorist group;[83] engaging in conspiracy to commit a terrorist act within or outside Nigeria;[84]aiding or abetting the commission of terrorist act;[85] attempts to commit an act of terrorism;[86] making preparations to commit an act of terrorism;[87] tampering with evidence related to the commission of a terrorist act;[88] and obstructing an authorized law enforcement officer in the exercise of powers under the Act.[89]

The Terrorism (Prevention) Act also imposes obligations on financial institutions and designated non-financial institutions to forward reports of suspicious transactions that relate to terrorist activities to the Nigerian Financial Intelligence Unit.[90] In addition, the Act establishes procedural measures to govern mutual assistance and extradition requests on terrorism-related offences.[91] Procedural powers under the Act include the powers of an authorized security or law enforcement agency to conduct investigations into terrorist activities.[92] For example, a duly authorized law enforcement agency can make an *ex parte* application to a Judge of the Federal High Court for an order to carry out the interception of communications in order to enable the prevention or detection of terrorist acts, or the prosecution of such acts.[93] Under the Act, the Federal High Court (following an *ex parte* application by a law enforcement authority) may grant an order for the detention of a person who is

71 *See* Section 4 Terrorism (Prevention) (Amendment) Act 2013.
72 *See* Section 5 Terrorism (Prevention) (Amendment) Act 2013.
73 *See* Section 6 Terrorism (Prevention) (Amendment) Act 2013.
74 *See* Section 7 Terrorism (Prevention) (Amendment) Act 2013.
75 *See* Section 8 Terrorism (Prevention) (Amendment) Act 2013.
76 *See* Section 9 Terrorism (Prevention) (Amendment) Act 2013.
77 *See* Section 10 Terrorism (Prevention) (Amendment) Act 2013.
78 *See* Section 11 Terrorism (Prevention) (Amendment) Act 2013.
79 *See* Section 12 Terrorism (Prevention) (Amendment) Act 2013.
80 *See* Section 13 Terrorism (Prevention) (Amendment) Act 2013.
81 *See* Section 14 Terrorism (Prevention) (Amendment) Act 2013.
82 *See* Section 15 Terrorism (Prevention) (Amendment) Act 2013.
83 *See* Section 16 Terrorism (Prevention) (Amendment) Act 2013.
84 *See* Section 17 Terrorism (Prevention) (Amendment) Act 2013.
85 *See* Section 18 Terrorism (Prevention) (Amendment) Act 2013.
86 *See* Section 20 Terrorism (Prevention) (Amendment) Act 2013.
87 *See* Section 21 Terrorism (Prevention) (Amendment) Act 2013.
88 *See* Section 23 Terrorism (Prevention) (Amendment) Act 2013.
89 *See* Section 24 Terrorism (Prevention) (Amendment) Act 2013.
90 *See* Section 14 Terrorism (Prevention) Act 2011.
91 *See* Sections 18-23 Terrorism (Prevention) Act 2011.
92 *See* Sections 24 and 25 Terrorism (Prevention) (Amendment) Act 2013.
93 *See* Section 29(1) Terrorism (Prevention) (Amendment) Act 2013.

suspected to have committed an act of terrorism for a period not exceeding 90 days, subject to the renewal of such an order pending the conclusion of the investigation and prosecution of the matter.[94]

Some scholars have criticized the provision of the 90 days detention order as being contrary to the right to personal liberty under section 35 (4) of the Constitution of the Federal Republic of Nigeria (1999)[95] which provides that:

"Any person who is arrested or detained…shall be brought before a court of law within a reasonable time, and if he is not tried within a period of –

(a) two months from the date of his arrest or detention in the case of a person who is in custody or is not entitled to bail; or

(b) three months from the date of his arrest or detention in the case of a person who has been released on bail, he shall (without prejudice to any further proceedings that may be bought against him) be released either unconditionally or upon such conditions as are reasonably necessary to ensure that he appears for trial at a later date".[96]

Although on the face of it such criticism may seem to be correct, he right to personal liberty under the Constitution is however not absolute. The right is limited under section 45(1) of the Constitution which provides that fundamental rights including the right to personal liberty can be restricted or derogated by "any law that is reasonably justifiable in a democratic society in the interest of defense, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedom of other persons".[97] This limitation implies that the exercise of the right to personal liberty has to be balanced against public interests such as the need to protect public safety or assist law enforcement and security agencies in their efforts to apprehend criminals. Therefore, the 90 day detention order under section 27(1) of the Terrorism (Prevention) (Amendment) Act[98] can be justified under section 45(1) of the 1999 Constitution of the Federal Republic of Nigeria on the grounds of protecting public safety and assisting law enforcement and security agencies in their efforts to deter acts of terrorism.

Section 27(3) of the Terrorism (Prevention) Act empowers law enforcement agencies to detain persons "found on any premises" pending the completion of search or investigation on such premises.[99] However, this provision appears problematic because it does not prescribe any time limits on the detention of arrested suspects. The Act also provides for the protection of witnesses[100] and persons who have volunteered information to a security or law enforcement agency for the purpose of investigating or prosecuting a terrorism offence.[101]

Charitable organizations are subject to regulation under the Terrorism (Prevention) Act. Such regulation aims to prevent the use of charitable organizations for the purpose of facilitating terrorist acts or rendering support to a terrorist group. For example, under section 35 (1) of the Act, the Registrar

94 *See* Section 27(1) Terrorism (Prevention) (Amendment) Act 2013.

95 *See* Olayinka Ajala and Eghosa O. Ekhator, 'Anti-Terrorism Law and the Protection of Human Rights in Nigeria: A Needless Conundrum?', *UNIPORT Law Review*(2017) Vol.1, pp.109-110. *See also*, A. T. Akujobi 'An Assessment of the Nigerian Terrorism Prevention Act and its Impact on National Security', *Global Journal of Human Social Sciences* (2018) Vol.18 (1), p.34.

96 *See* Section 35 (4) Constitution of the Federal Republic of Nigeria (1999).

97 *See* Section 45(1) Constitution of the Federal Republic of Nigeria (1999).

98 *See* Section 27(1) Terrorism (Prevention) (Amendment) Act 2013.

99 *See* Section 27(3) Terrorism (Prevention) (Amendment) Act 2013.

100 *See* Section 34 Terrorism (Prevention) (Amendment) Act 2013.

101 *See* Section 33 Terrorism (Prevention) (Amendment) Act 2013.

General of the Corporate Affairs Commission may refuse to register a charitable organization or revoke the registration of such an organization where, based on security or criminal intelligence reports, there are reasonable grounds to believe that an applicant for the registration of a charity or a registered charity has made, or is making, or is likely to make available any resources directly or indirectly to a terrorist group.[102] However, a registered charity or person that has been affected by such revocation or refusal of registration can make an application for judicial review before a Federal High Court.[103]

The Office of the National Security Adviser coordinates all security and law enforcement agencies with respect to the enforcement of the Terrorism (Prevention) Act.[104] The Office's responsibilities include: providing support to all relevant security/intelligence, law enforcement agencies and military services to prevent and combat acts of terrorism in Nigeria; ensuring the effective formulation and implementation of a comprehensive counter terrorism strategy in Nigeria; and, building capacity to enhance the effective discharge of the functions of security/intelligence, law enforcement and military services under the Terrorism (Prevention) Act and any other Nigerian law on terrorism.[105] On the other hand, the Attorney General of the Federation is responsible for ensuring the effective implementation and administration of the Act and also for strengthening Nigeria's existing legal framework on counter terrorism to ensure the effective prosecution of terrorism matters and ensuring Nigeria's compliance with international standards and United Nations conventions on terrorism.[106]

3.2 The Economic and Financial Cries Commission (Establishment) Act

The Economic and Financial Crimes Commission (Establishment) Act criminalizes offences relating to economic and financial crimes[107] and 'terrorism'.[108] The Act is currently the only Nigerian law that explicitly defines 'terrorism'[109] and further criminalizes acts or attempts to commit or facilitate the commission of a terrorist act.[110] It also prohibits acts that relate to the financing of terrorism. In this regard, the Act criminalizes the willful provision or collection of money from persons with the intent or knowledge that such money will be used for any act of terrorism.[111] The Act also criminalizes the provision of funds, financial assets or economic resources or financial services available to any person

[102] *See* Section 35 (1) Terrorism (Prevention) Act 2011.
[103] *See* Section 35 (4) - (8) Terrorism (Prevention) Act 2011.
[104] *See* Section 1 A (1) Terrorism (Prevention) (Amendment) Act 2013.
[105] *See* Section 1 A (1) Terrorism (Prevention) (Amendment) Act 2013.
[106] *See* Section 1 (2) Terrorism (Prevention) (Amendment) Act 2013.
[107] *See* Part IV Economic and Financial Crimes Commission (Establishment) Act 2004.
[108] *See* Section 15 Economic and Financial Crimes Commission (Establishment) Act 2004.
[109] Under section 46 of the Act 'terrorism' is defined as:
"(a) Any act which is a violation of the Criminal Code or the Penal Code and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to any person, any member or group of persons, or causes or may cause damage to public or property, natural resources, environmental or cultural heritage and is calculated or intended to – intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act or to adopt or abandon a particular standpoint, or to act according to certain principles, or disrupt any public service, the delivery of any essential service to the public or to create a public emergency, or create general insurrection in a State;
(b) any promotion, sponsorship of, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organization or procurement of any person, with the intent to commit any act referred to in paragraph (a) (i), (ii) and (iii)".
[110] *See* Section 15 (2) Economic and Financial Crimes Commission (Establishment) Act 2004.
[111] *See* Section 15 (1) Economic and Financial Crimes Commission (Establishment) Act 2004.

for the purpose of facilitating the commission of a terrorist act.[112] Under the Act, the Economic and Financial Crimes Commission is responsible for adopting measures to identify, trace, freeze, confiscate or seize proceeds relating to terrorist activities[113] including funds destined for Boko Haram.

3.3 The Money Laundering (Prohibition) Act

The Money Laundering (Prohibition) Act criminalizes the laundering of any fund or property that is "part of the proceeds of an unlawful act".[114] Under the Act, "an "unlawful act" includes participating in an act of terrorism or terrorist financing.[115] In order to prevent the laundering of funds for the purpose of promoting terrorism and other unlawful acts, the Act prescribes the limit of cash transactions that can be made outside a financial institution by a person or corporate body.[116] The Act also imposes obligations on banks and financial institutions to identify their customers[117] and report international funds transfers exceeding $10,000,[118] as well as suspicious financial transactions that relate to terrorist financing.[119]

3.4 The National Security Strategy

The National Security Strategy was established by the Nigerian government in November, 2014 to set out Nigeria's national security vision. The strategy identifies Nigeria's national security threats to include challenges such as terrorism and ethno-religious conflicts and prescribes strategies to address those challenges.[120] In particular, the strategy states that the effects of Boko Haram's violent activities include: mass displacements and forced migration of populations; the undermining of agriculture and other economic activities; the exacerbation of community tensions; and the proliferation of small arms and light weapons.[121] In order to provide effective responses to the violent activities of terrorist groups such as Boko Haram, the strategy prescribes five core elements to promote counter terrorism. These five elements include (i) identifying terrorists and their sponsors and bringing them to justice; (ii) preparing the Nigerian populace so as to mitigate the consequences of terrorists incidents; (iii) forestalling and preventing terrorism by engaging the Nigerian public through sustained education and de-radicalization programmes; (iv) ensuring the security of lives and property, including national infrastructure and services; and, (v) devising a framework to effectively mobilize and sustain cross-governmental efforts in the implementation of Nigeria's counter terrorism strategy.[122]

The National Security Strategy recognizes that applying only a military approach will not effectively counter ideology based terrorist insurgencies such as the Boko Haram. Therefore, the

---

[112] *See* Section 15 (3) Economic and Financial Crimes Commission (Establishment) Act 2004.
[113] *See* Section 6 (d) Economic and Financial Crimes Commission (Establishment) Act 2004.
[114] *See* Section 15 (2) Money Laundering (Prohibition) Act 2011.
[115] *See* Section 15 (6) Money Laundering (Prohibition) Act 2011.
[116] *See* Section 1 Money Laundering Prohibition Act 2011.
[117] *See* Section 3(1) Money Laundering (Prohibition) Act 2011.
[118] *See* Section 2(1)-(2) Money Laundering (Prohibition) Act 2011.
[119] *See* Section 6 (1) (d) Money Laundering (Prohibition) Act 2011. For an analysis of the obligations of banks and financial institutions under the Act, *see* Uchenna Jerome Orji, 'A Review of the Special Duties of Banks under the Nigerian Money Laundering Act', *Journal of International Banking Law and Regulation* (2011) Vol. 26, (6) pp. 299-305.
[120] *See* Federal Republic of Nigeria, *National Security Strategy* (November, 2014).
[121] *Ibid*, pp.14-15.
[122] *Ibid*, pp.30-31.

strategy establishes a "Soft Approach" to counter terrorism.[123] The soft approach is designed to involve Local Governments, State Governments, civil society organizations including religious organizations and the private sector. The approach also involves the design and implementation of prison-based de-radicalization programmes for persons convicted under the Terrorism (Prevention) Act and for suspects awaiting trial for terrorism offences.[124] A major objective of the soft approach is to undertake the reformation and rehabilitation of persons convicted of terrorism in order to prepare such individuals for a possible re-entry into the society. The soft approach also advocates an over-haul of the educational system in northern Nigeria with a view to promoting the entrenchment of critical thinking at the core of the educational system so as to steer vulnerable youth away from the misguided interpretation of religious texts[125] and thereby minimize the potential for their radicalization by clerics. Another element of the soft approach is that it proposes the implementation of an economic revitalization programme in States most affected by the terrorist activities of Boko Haram.[126] This aims to ensure that people in such areas are economically engaged so as to minimize unemployment and poverty.

3.5 The National Counter Terrorism Strategy

The Office of the National Security Adviser originally developed the Nigerian National Counter Terrorism Strategy in 2014. A revised version of the Strategy was adopted by the Nigerian government in August, 2016.[127] The Strategy aims to achieve five major objectives which are: forestalling the emergence of terrorists and support for terrorism; securing citizens and infrastructure against terrorist attacks; identifying and disrupting acts of terrorism; preparing responses to manage and mitigate terrorist attacks; and implementing a framework for mobilizing coordinated public and private sectors to counter terrorism.

The Office of the National Security Adviser is responsible for coordinating the implementation of the National Counter Terrorism Strategy,[128] while the Federal Ministry of Justice is required to develop the capacity of the criminal justice system to efficiently deal with terrorism cases by facilitating the speedy prosecution of persons being tried for terrorism and also working with relevant institutions to introduce a legislation that will criminalize the incitement and recruitment of terrorists in places of religious worship and training.[129]

3.5 The Policy Framework and National Action Plan for Preventing and Countering Violent Extremism

The Policy Framework and Nation Action Plan for Preventing and Countering Violent Extremism was established by the Nigerian government in August, 2017, to address the short, medium and long term objectives for tackling violent extremism in Nigeria.[130] The Framework aims to achieve

[123] *See* Federal Republic of Nigeria, *National Security Strategy* (November, 2014) pp.32-33.
[124] *Ibid*.
[125] *Ibid*.
[126] *Ibid*, pp.34-35.
[127] *See* Office of the National Security Adviser, *The National Counter Terrorism Strategy (Revised)* (2016).
[128] *Ibid*, p.49.
[129] *See* Office of the National Security Adviser, *The National Counter Terrorism Strategy (Revised)* (2016), p.42.
[130] *See* Federal Republic of Nigeria, *Policy Framework and National Action Plan for Preventing and Countering Violent Extremism* (August, 2017).

objectives that include: (i) institutionalizing and coordinating programmes for preventing and countering violent extremism at the national, state and local government levels;[131] (ii) strengthening access to justice and promoting respect for human rights and the rule law; and (iii) enhancing the capacity of individuals and communities to prevent and counter violent extremism and also recover from acts of violent extremism.[132] In order to effectively tackle violent extremism in Nigeria, the Framework provides for the establishment of strong partnerships between the government and other critical stakeholders including youths, students, women and girls, schools and teachers, community leaders, leaders of religious organizations, social workers, civil society organizations, media and social media influencers, social mobilizers, political leaders, the Police, the private sector and the military.[133] The Framework also recognizes that effectively countering violent extremism in Nigeria requires the implementation of community policing approaches, and improved civil-military relations.[134]

More importantly, the Framework prescribes measures to strengthen rule of law, as well as access to justice and the protection of human rights in countering violent extremism. In this respect, the Framework promotes the reform of legal frameworks and policies on countering violent extremism where necessary so as to enhance the protection of human rights and access to justice.[135] The Framework also aims to strengthen the competencies of security/intelligence and law enforcement agencies, as well as judicial authorities with a view to enhancing effective crime prevention and respect for human rights and rule of law, and thereby reducing the occurrence of grievances that can lead to violent extremism.[136] The Office of the National Security Adviser is responsible for coordinating and monitoring the implementation of the Framework and also collaborating with stakeholders in ensuring its effective implementation.[137]

4. Challenges Impeding the Enforcement of Nigeria's Counter Terrorism Regime and Proposals for Responses

To a large extent, Nigeria's counter terrorism regime appears to meet basic standards for tackling acts of terrorism. However, there are peculiar challenges that hinder its application against Boko Haram. Such challenges include: inefficient handling of terrorism cases resulting in the prolonged detention of suspects without trial, poor investigation of cases, lack of effective synergy between the military and the Federal Ministry of Justice, logistical challenges, the use of informal channels for terrorist financing activities and the inability of the government to address the root causes of violent religious extremism such as poverty, unemployment and inequality. In this section, the paper will discuss how these challenges impede the enforcement of Nigeria's counter terrorism measures in curbing Boko Haram's activities and propose responses in that regard.

---

131 *Ibid*, p.12.
132 *Ibid*, pp.12-13.
133 *Ibid*, pp.17-24.
134 *Ibid*, p.24.
135 *See* Federal Republic of Nigeria, *Policy Framework and National Action Plan for Preventing and Countering Violent Extremism* (August, 2017), p.27.
136 *Ibid*, p.27.
137 *Ibid*, p.25.

4.1 Inefficient Handling and Prosecution of Boko Haram Cases

Nigeria's war against Boko Haram has resulted in the arrest and capture of a significant number of persons alleged to be members of the sect. However, there have not been commensurate efforts to ensure the speedy prosecution of those persons before competent courts of law so as to facilitate their conviction and punishment under Nigeria's counter terrorism laws. A report by Human Rights Watch observes that:

"since 2009 security forces have arrested thousands of people suspected of involvement in Boko Haram's violence. However, the whereabouts of a large majority of those arrested are unknown; others are detained by security forces in military detention facilities for prolonged periods without trial".[138]

For example, it has been reported that about 5000 to 10,000 persons who are alleged to Boko Haram members are being held in several prisons across Nigeria. Out of that number, about 3000 Boko Haram case files are pending in various courts across Nigeria with many of the cases bordering on the alleged violation of the fundamental human rights of the detainees who claim to have been erroneously arrested and held by security agencies without trial.[139] Also, out of the over 3000 pending case files, around 1000 are core terrorism trials that are still pending before the courts, with only very few cases being concluded at the High Courts.[140] A report by the Nigerian Stability and Reconciliation Programme observes that "there has been minimal success in the prosecution of members of the [Boko-Haram] terrorist sect".[141] The report further notes that between 2009 and 2016, there were 939 Boko Haram cases at the trial stage with only one conviction recorded.[142] Another report observes that the Federal Government has concluded thirteen criminal trials involving Boko Haram members, from which it has secured nine convictions.[143] While there are several different reports regarding the actual number of Boko Haram members that have been convicted by the courts,[144] the poor prosecution of Boko Haram cases has, however, been traced to several factors, including lack of evidence to facilitate prosecution, lack of legal representation for defendants, an absence of prosecutors, and the transfer of defendants to unknown locations outside the jurisdiction of courts during periods of trial.[145]

The poor prosecution of suspected Boko Haram members creates the potential for other challenges that compound Nigeria's counter terrorism efforts. For example, the poor prosecution of such cases can engender a loss of confidence in the criminal justice system. In this regard, individuals or communities who have been affected by Boko Haram's violent extremism tend to lose hope in the criminal justice system and in the ability of the State to protect them and provide justice. A survey conducted under

---

[138] *See* Human Rights Watch, *Those Terrible Weeks in their Camp – Boko Haram Violence Against Women and Girls in North-east Nigeria* (Human Rights Watch: United States of America, 2014) p.47.

[139] *See* John Chuks Azu, 'Over 3000 Boko Haram Cases Stall in Courts', *Daily Trust* (10 September, 2017), available at <https://www.dailytrust.com.ng/over-3-000-boko-haram-case-stall-in-courts.html> last accessed on 16 January 2020.

[140] *Ibid*.

[141] *See* Nigerian Institute of Advanced Legal Studies, *Dealing with the Past: Justice, Reconciliation and Healing in the North East of Nigeria* (Nigeria Stability and Reconciliation Programme: Abuja, Nigeria, 2017) p. 37.

[142] *Ibid*.

[143] *See* Ikechukwu Nnochiri, 'FG Okays Trial of 1,600 Alleged Boko Haram Terrorists, Frees 220 Suspects', *Vanguard* (24 September, 2017), available at <https://www.vanguardngr.com/2017/09/fg-okays-trial-1600-alleged-boko-haram-terrists-frees-220-suspects/> last accessed on 16 January 2020.

[144] *See* Nigerian Institute of Advanced Legal Studies, *ibid*, p.37; Human Rights Watch, *Those Terrible Weeks in their Camp – Boko Haram Violence Against Women and Girls in Northeast Nigeria* (Human Rights Watch: United States of America, 2014) p.48.

[145] *See* Human Rights Watch, *ibid*, p.47.

the Nigeria Stability and Reconciliation Programme found that people in communities affected by Boko Haram's violence were dissatisfied with how Boko Haram cases were handled and believed that there was no political will to prosecute the sect's members and therefore had little confidence in the judiciary and justice system.146 Another negative implication of the poor prosecution of Boko Haram cases is that it also creates excuses that can be used by security forces and law enforcement agencies to unlawfully detain terror suspects for very long periods without trial and to justify summary executions or the extra judicial killings of suspected terrorists.147 Another challenge is that the prolonged detention of suspects due to the poor prosecution of cases can expose detained innocent suspects to Boko Haram's radicalization during the period of detention. This can, therefore, create a situation whereby innocent persons who have been detained without prosecution for long periods on suspicion of having committed acts of terrorism become radicalized during the period of their detention, thus increasing the ranks of Boko Haram when they are eventually released into the society.

In order to address the poor prosecution of Boko Haram cases, there is a need for a careful exercise of the detention powers under section 27(1) of the Terrorism (Prevention) (Amendment) Act 2013. In this regard, the courts will have to carefully consider ex parte applications brought by law enforcement agencies for the prolonged detention of arrested Boko Haram suspects pending the investigation and prosecution of the matter that led to their arrest and detention. For example, it would be helpful if the courts were to grant prolonged detention orders after considering that there is a substantial evidence and an overriding need that justifies the prolonged detention of arrested Boko Haram suspects pending the conclusion of investigations by law enforcement agencies and the prosecution of such cases. In this regard, a relevant element that should provide basis for a court to grant such an order for the prolonged detention of an arrested suspect is whether such order will actually prevent interference with the investigation and prosecution of a terrorism case. Furthermore, the court should also take into cognizance whether the relevant law enforcement authority have consistently demonstrated diligence in the investigation and prosecution of matters for which applications for prolonged detention of Boko Haram suspects have been made. This will help to ensure that the excuse of carrying out the investigation and prosecution of arrested Boko Haram suspects is not used by law enforcement authorities to justify the indefinite detention of suspects without actually carrying out a diligent investigation and prosecution of the matters that led to their arrest and detention in the first place.

There is also need for a review of section 27(3) of the Terrorism (Prevention) (Amendment) Act (2013) in order to subject the powers of a law enforcement agency to detain persons found on any premises pending the completion of a search or investigation to judicial review. This is imperative because there is no requirement for either judicial authorization or judicial review of the detention powers under section 27(3) of the Terrorism (Prevention) (Amendment) Act (2013), and neither does the section prescribe any time limits on the detention of arrested suspects.

Another measure that is necessary to address the poor prosecution of arrested Boko Haram suspects is for the Federal Ministry of Justice to develop a justice administration policy that will facilitate the expeditious prosecution of terrorism cases. Security forces engaged in countering the

146 *See* Nigerian Institute of Advanced Legal Studies, *Dealing with the Past: Justice, Reconciliation and Healing in the North East of Nigeria* (Nigeria Stability and Reconciliation Programme: Abuja, Nigeria, 2017) p.37.

147 *See* Amnesty International, *Nigeria: Trapped in the Cycle of Violence* (Amnesty international: London, United Kingdom, 2012) pp.18-28.

terrorist activities of Boko Haram have noted the absence of an articulated policy by the Federal Ministry of Justice to enhance the expeditious prosecution of arrested Boko Haram suspects as one of the major factors responsible for the prolonged detention of suspects.[148] Therefore, the Ministry of Justice's development of an effective policy on the prosecution of Boko Haram suspects will enhance the profiling of arrested suspects so as to facilitate their timely release from detention or their speedy prosecution and conviction.

There is also need to build capacity in the Federal Ministry of Justice by recruiting more prosecutors so as to ensure that the increasing number of Boko Haram cases in various courts across the country does not overwhelm the Ministry. This will make the Ministry more capable to effectively prosecute Boko Haram cases and also minimize situations whereby the absence of prosecutors would impede trials. In addition, the enhancement of the capacity of judiciary to try matters involving suspected Boko Haram members is imperative. Under the Terrorism (Prevention) (Amendment) Act only the Federal High Court has the jurisdiction to try cases relating to terrorism.[149] However, most States in Nigeria have only one division of the Federal High Court with a limited number of Judges. This also delays the prosecution of Boko Haram cases as the Federal High Courts may have fewer Judges trying many Boko Haram cases, thereby resulting in prolonged trial periods. The problem is further compounded by the absence of special courts to try terrorism cases in Nigeria.

Therefore, in order to address this challenge, there is need for more Judges to be employed and deployed to designated Federal High Courts for the purpose of facilitating the timely trial of Boko Haram cases. Another helpful alternative will be to establish special courts to try terrorism offences. This approach would eliminate several of the logistical factors that are responsible for the delay of Boko Haram cases and enhance the speedy trial of such cases.

4.2 Poor Investigation of Cases Involving Boko Haram Suspects

The effective enforcement of Nigeria's counter terrorism regime has also been impeded by the poor investigation of Boko Haram suspects. For example, it has been observed that most Boko Haram cases are being prosecuted on the basis of mere confessions with no independent corroborative evidence.[150] A report by Human Rights Watch notes that many victims of Boko Haram attacks have expressed frustration over lack of investigation of crimes committed against them by the sect, including perceived lack of interest and the failure of the police to interview them or document their complaints in order to identify the perpetrators.[151] However, without independent corroborative evidence, mere confessions by suspected Boko Haram members would not provide sufficient basis for conviction by courts, because the burden of proof must be discharged beyond reasonable doubt in criminal cases. This results in the stagnation of cases as well as the prolonged detention of Boko Haram suspects. A major factor that is responsible for the poor investigation of cases that involve Boko Haram suspects is the lack of skilled personnel and requisite technical capacities to enable the conduct of forensic criminal investigations

[148] *See* John Chuks Azu, 'Over 3000 Boko Haram Cases Stall in Courts', *Daily Trust* (10 September, 2017), available at <https://www.dailytrust.com.ng/over-3-000-boko-haram-case-stall-in-courts.html> last accessed on 16 January 2020.

[149] *See* Section 32 (1)-(2) Terrorism (Prevention) (Amendment) Act 2013.

[150] *See* John Chuks Azu, *ibid*.

[151] *See* Human Rights Watch, *Those Terrible Weeks in their Camp: Boko Haram Violence against Women and Girls in North-east Nigeria* (Human Rights Watch: United States, 2014) p.49. *See also* Amnesty International, *Nigeria: Trapped in the Cycle of Violence* (Amnesty International: United Kingdom, 2012) pp. 45-46.

by law enforcement authorities, especially the Nigerian Police.[152] Therefore, in order to address the poor investigation of cases involving Boko Haram suspects, it is imperative that the capacity of the Nigerian Police to carry out investigations on terrorism cases be improved. This requires providing the Police with the necessary equipment for securing and examining crime scenes, including the conduct of ballistics and other forensic tests such as autopsies and medical examinations. In addition, there is need to train skilled forensic personnel that will carry out complex investigations required to gather adequate evidence that can be used to prosecute and convict Boko Haram suspects.[153]

4.3 Lack of Synergy between the Military and Federal Ministry of Justice

The Nigerian government appears to have focused more on enhancing the capacities of the military to fight Boko Haram. Hence, when compared to the Police and other security agencies, the military appears better trained, equipped and funded to provide immediate response to the Boko Haram challenge.[154] Consequently, the military has consistently been at the forefront of tackling Boko Haram's terrorist activities. This has led to the military increasingly carrying out law enforcement functions and exercising police powers,[155] including the arrest and detention of Boko Haram suspects.[156] However, the military does not have the powers to prosecute Boko Haram suspects. The responsibility for prosecuting such suspects is vested in the office of the Director of Public Prosecutions within the Federal Ministry of Justice[157] which commences prosecution by filing an Information or Charge against a suspect in the Federal High Court.[158] Therefore, ensuring the effective prosecution of Boko Haram suspects who have been arrested by the military requires the existence of an effective synergy between the military and Ministry of Justice. The absence of such synergy has created challenges in terms of converting military intelligence that led to the arrest and detention of Boko Haram suspects into admissible evidence that can be used to conduct criminal trials and secure convictions in a court of law. This has led to the stagnation of Boko Haram cases at detention centers without being brought to trial before courts of law.[159]

In order to address the challenge of lack synergy between the Ministry of Justice and the military, there is need to create a platform that will build effective synergy between the two institutions, so as to enhance the gatthering of admissible evidence against Boko Haram suspects arrested by the military. In

[152] *See* Noel Otu and Oko Elechi, 'The Nigeria Police Forensic Investigation Failure', *Journal of Forensic Sciences & Criminal Investigation* (May, 2018), Vol. 9 (1), pp.1-7.

[153] *See* Jason Burke, 'Secret Trials of Thousands of Boko Haram Suspects to Start in Nigeria', *The Guardian* (9 October, 2017), available at <https://www.theguardian.com/world/2017/oct/09/nigeria-begin-secret-trials-thousands-boko-haram-suspects> last accessed on 16 January 2020.

[154] *See* Jude Egbas, 'Security Challenge: How Nigerian Army is Taking over the Job of the Police', Pulse Nigeria (4 October, 2018), available at <https://www.pulse.ng/news/local/how-nigerian-army-is-taking-over-job-of-the-police-id8205276.html> last accessed on 16 January 2020.

[155] *See* Matthew T. Page, 'Nigeria Struggles with Sector Reform', Chatham House Experts Comments (2 April, 2019), available at <https://www.chathamhouse.org/expert/comment/nigeria-security-sector-reform> last accessed on 16 January 2020.

[156] *See* Amnesty International, *Nigeria: Trapped in the Cycle of Violence* (Amnesty International: United Kingdom, 2012) p. 49; Peterside Zainab Brown, 'The Military and Internal Security in Nigeria: Challenges and Prospects', Mediterranean Journal of Social Sciences (2014), Vol. 5, No.27, pp.1301-1306; Jude Egbas, 'Security Challenge: How Nigerian Army is Taking over the Job of the Police', Pulse Nigeria (4 October, 2018).

[157] *See* section 106 (a) Administration of Criminal Justice Act.

[158] *See* Section 109 *ibid*.

[159] *See* Ikechukwu Nnochiri, 'FG Okays Trial of 1,600 Alleged Boko Haram Terrorists, Frees 220 Suspects', *Vanguard* (24 September, 2017), available at <https://www.vanguardngr.com/2017/09/fg-okays-trial-1600-alleged-boko-haram-terrists-frees-220-suspects/> last accessed on 16 January 2020.

2017, the Attorney General of the Federation set up a coordinating center and investigating unit for all criminal cases arising from offences created by Acts of the National Assembly on the basis of section 105 of the Administration of Criminal Justice Act (2015).[160] While this step is highly commendable, it is, however, imperative that such a platform is effectively utilized for the purpose of working with the military to gather admissible evidence that can be used to prosecute Boko Haram suspects.

4.4 The Challenge of Tracking and Freezing Boko Haram's Finances

One major challenge in enforcing Nigeria's counter terrorism measures against Boko Haram is the difficulty in tracking the sect's finances so as to apply freezing measures. This challenge arises from the fact that Boko Haram does not utilize formal channels for financing its activities. Major sources of Boko Haram's funding include armed robberies, kidnappings for ransom, extortions, funding from sympathizers, illegal trafficking of fire arms and fees from members. Most funding from the above sources are not channeled through the formal banking and financial system as Boko Haram uses couriers to move cash throughout northern Nigeria.[161] This makes it is difficult for law enforcement authorities to track the sect's funding in order to apply freezing measures under Nigeria's counter terrorism laws. To some extent, this challenge can be addressed by improving the capacity of law enforcement agencies to effectively gather intelligence on the sources of Boko Haram's finances and how such funds are transmitted through informal channels so as identify and dismantle such channels and starve the sect of funds.

4.5 Inadequate Responses towards Addressing the Root Causes of Boko Haram's Violent Extremism

There are several factors that have been identified as the root causes of Boko Haram's violent extremism in northern Nigeria. Such factors include widespread poverty and inequality, massive unemployment, high levels of illiteracy, widespread corruption, and the heavy handed approach of security forces in suppressing manifestations of militant Islamism.[162] The persistent manifestation of these factors will continue to challenge and impede Nigeria's counter terrorism efforts against Boko Haram. However, the government appears not to have provided adequate responses to the above challenges. For example, a United Nations Development Programme (UNDP) Human Development report indicates that Nigeria has a very low human development index[163] and one of the highest rates of poverty in the world (with about 54.8 percent of the country's population classified as being in multidimensional poverty, while 30 percent of the country's population is classified as being in "*severe* multidimensional poverty").[164] Reports from Nigeria's National Bureau of Statistics (NBS)

[160] *See* John Chuks Azu, 'Over 3000 Boko Haram Cases Stall in Courts', *Daily Trust* (10 September, 2017), available at <https://www.dailytrust.com.ng/over-3-000-boko-haram-case-stall-in-courts.html> last accessed on 16 January 2020.

[161] *See* Jason L. Rock, *The funding of Boko Haram and Nigeria's Actions to Stop It* (A Master of Science submitted to the United States Naval Postgraduate School (California: December, 2016) p.16.

[162] *See* Freedom C. Onuoha, 'Why do Youth Join Boko Haram', *United States Institute of Peace Special Report* (June, 2014) No. 345, pp.5-7.

[163] *See* The United Nations Development Programme (UNDP), *Human Development Report 2016: Human Development for Everyone* (UNDP: New York, USA, 2016), pp.200, 204,208, 212, 216, & 271.

[164] *Ibid*, p.219 (Emphasis added). The UNDP Human Development Report (2015) also classifies Nigeria as one of the five countries with the largest population of people in multidimensional poverty. *See* UNDP, *Human Development Report 2015* (UNDP: New York, USA, 2015) p.61.

also indicate that relative poverty was most apparent in States in the north-eastern region of Nigeria, with a poverty rate of 76.3%.[165] Such high poverty rates create deep inequalities in terms of access to education, healthcare, justice, and other basic services, and also increases the levels of resentment against the government. This state of affairs, coupled with massive youth unemployment and low literacy rates, makes youths vulnerable to radicalization and extremist religious views.[166] Even though it may be argued that unemployment and poverty are not the main factors that influence Boko Haram's ability to radicalize young people in Nigeria, it has been observed that "the tendency to produce suicide bombers is greater in a community defined by mass misery and joblessness than the one in which basic needs of food, education, health, housing, and sanitation are met for the majority of the people".[167] Therefore, given this reality, it is imperative that the government effectively addresses factors that are responsible for poverty, inequality, illiteracy and massive unemployment in the north-eastern region of Nigeria so as to reduce vulnerability of the youth to radicalization.

The inability of the Nigerian government to effectively tackle corruption amongst public officials also feeds Boko Haram's rhetorical narrative that the application of strict and conservative Sharia laws will address social ills and injustice within Muslim communities in northern Nigeria. Thus, widespread corruption in Nigeria has deprived communities of essential services and infrastructure, while also creating an enabling environment for Boko Haram recruitment and radicalization.[168] Therefore, in order to tackle Boko Haram's narrative that the application of strict and conservative Sharia law will address social ills and injustice within Muslim communities in northern Nigeria, there is need for the government to effectively tackle corruption, especially in the public sector so as to ensure the promotion of the public good and prevent the rise of social grievances that encourage radicalization or support for Boko Haram.

There is also need for the government to effectively hold security forces accountable for incidents of excessive use of force and human rights violations during counter terrorism operations so as to minimize collateral damage to innocent civilians and loss of public confidence due to the deployment of harsh operational tactics. As noted earlier, one of the factors that led to the transformation of Boko Haram into a very dangerous and violent Islamist sect was the outcome of the harsh operational tactics which were deployed by security forces to contain the 2009 Boko Haram uprising.[169] This included cold blooded extra judicial killings (such as the execution of the sect's leader and captured members), dragnet arrests, extortion, unlawful confiscation of properties belonging to alleged Boko Haram members and sympathizers and intimidation of the local population.[170] However, there has not been significant effort on the part of the government towards holding the personnel of security forces accountable for such excessive use of force during counter terrorism operations. For example, the outcome of the Panel of Inquiry that was set up to probe the circumstances that led to the extra-

[165] *See* BBC, 'Nigerians Living in Poverty Rise to Nearly 61 Percent', *BBC News* (13 February, 2012), available at <http://www.bbc.com/news/world-africa-17015873> last accessed on 16 January 2020.

[166] *See* Usman Solomon Ayegba, 'Unemployment and Poverty as Sources and Consequence of Insecirity in Nigeria: The Boko Insurgency Revisited', *African Journal of Political Science and International Relations* (2015), Vol.9 (3), pp.90-98.

[167] *See* Kayode Komolafe, 'Boko Haram: A Crisis in Search of Strategy', *Thisday* (25 January, 2012), p. 56. *See also* Freedom C. Onuoha, 'Why do Youth Join Boko Haram', *United States Institute of Peace Special Report* (June, 2014) No. 345, p.6.

[168] *See* Freedom C. Onuoha, *ibid* at p.7.

[169] *See* James J.F. Forest, *Confronting the Terrorism of Boko Haram in Nigeria* (Joint Special Operations University Press, Florida, United States, 2012) p.64, and Foard Copeland, *The Boko Haram Insurgency in Nigeria* (The Civil – Military Fusion Centre, February, 2013) p.3.

[170] *Ibid*.

judicial killing of Mohammed Yusuf and captured Boko Haram members in 2009 did not result in significant indictments or the imposition of sanctions on the personnel of security forces that were involved in the killings. The government was also unable to successfully prosecute and convict four policemen for allegedly killing Mohammed Yusuf.[171]

This of affairs fuels local resentment against the Nigerian government and contributes in swelling Boko Haram's ranks with new members and sympathizers,[172] and further compounds Nigeria's counter terrorism efforts by making it difficult for local populations to cooperate with security forces and law enforcement agencies in deterring or prosecuting acts of terrorism. However, to a large extent, promoting the accountability of security forces and law enforcement agencies in counter terrorism operations and ensuring the rule of law and human rights protection during such operations will reduce the potential for the excessive use of force and human right violations. Such measures may also prevent individuals who have been victims of excessive use of force and human right violations from seeking self-help or vengeance against the personnel of security forces or giving sympathy to Boko Haram. More importantly, such measures will help to restore public confidence in the ability of the government to check the excesses of security forces engaged in counter terrorism operations.

5. Concluding Remarks

Countering the terrorist activities of Boko Haram remains a serious national security challenge for Nigeria. The Nigerian government has provided several responses towards addressing the challenge including legal and policy measures and the use of military operations. However, it appears that Nigerian government has largely applied a military solution in addressing the Boko Haram challenge. Sole reliance on the military approach will not yield sustainable outcomes. Although the military solution appears necessary in the short term in order to prevent Boko Haram from capturing territories and creating an Islamic State within the Nigerian State, the long term success of Nigeria's counter terrorism operations against the sect will be determined by other elements including the effective and accountable application of the existing counter terrorism laws and policies. Despite Nigeria's establishment of counter terrorism measures, it appears however that their effective application to curb Boko Haram's terrorist activities have been limited by several peculiar challenges which were identified in this paper. Therefore, to a large extent, the identified challenges clearly create gaps between Nigeria's counter terrorism regimes and their effective enforcement against Boko Haram, and thereby disconnecting existing counter terrorism regimes and actual counter terrorism efforts in practice. In the light of this state of affairs, it is therefore imperative that efforts are made to timely address the highlighted challenges so as to strengthen the application of Nigeria's counter terrorism regime to curb Boko Haram's terrorist activities.

---

[171] *See* AFP, 'Policemen Accused of Killing Boko Haram Founder Reinstated', *The Guardian* (19 February, 2018), available at <https://m.guardian.ng/news/policemen-accused-of-killing-boko-haram-founder-reinstated/> Roland Mutum and John Chuks Azu, 'Police Reinstate Officers Acquitted of Killing Boko Haram Leader', *Daily Trust* (19 February, 2018), available at <https://www.dailytrust.com.ng/police-reinstate-officers-acquitted-of-killing-Boko-haram-leader.html> last accessed on 16 January 2020.

[172] *See* Foard Copeland, *The Boko Haram Insurgency in Nigeria* (The Civil – Military Fusion Centre, February, 2013) p.3.

BIBLIOGRAPHY

Books/Chapters in Books

Forest, James J.F., *Confronting the Terrorism of Boko Haram in Nigeria* (Joint Special Operations University Press, Florida, United States, 2012).

Muhammad, Isa, 'Militant Islamist Group, in Northern Nigeria', in Wafula Okumu and Augustine Ikelegbe (eds) *Militias, Rebels and Islamic Militants: Human Insecurity and State Crises in Africa* (Institute for Security Studies: Pretoria).

Articles in Journals and Newspapers

Ajala, Olayinka, and Ekhator, Eghosa O., 'Anti-Terrorism Law and the Protection of Human Rights in Nigeria: A Needless Conundrum?', *UNIPORT Law Review*(2017) Vol.1.

Akujobi, A. T., 'An Assessment of the Nigerian Terrorism Prevention Act and its Impact on National Security', *Global Journal of Human Social Sciences* (2018) Vol.18 (1).

Ayegba, Usman Solomon, 'Unemployment and Poverty as Sources and Consequence of Insecirity in Nigeria: The Boko Insurgency Revisited', *African Journal of Political Science and International Relations* (2015), Vol.9 (3).

Brown, Peterside Zainab, 'The Military and Internal Security in Nigeria: Challenges and Prospects', Mediterranean Journal of Social Sciences (2014), Vol. 5, No.27.

Clarke, Stephen Buchana and Knoope, Peter, 'The Boko Haram Insurgency: From Short Term Gains to Long Term Solutions', *Institute for Justice and Reconciliation Occasional Paper* (January, 2017) No.23.

Copeland, Foard, *The Boko Haram Insurgency in Nigeria* (The Civil – Military Fusion Centre, February, 2013).

Falode, James Adewunmi, 'The Nature of Nigeria's Boko Haram War, 2010-2015: A Strategic Analysis', *Perspectives on Terrorism* (2016) Vol.10 (1).

Habibu Yaya Bappah, 'Nigeria's Military Failure against the Boko Haram Insurgency', *African Security Review* (2016) Vol. 25(8).

Noel Otu and Oko Elechi, 'The Nigeria Police Forensic Investigation Failure', *Journal of Forensic Sciences & Criminal Investigation* (May, 2018), Vol. 9 (1).

Onuoha, Freedom C., 'The Islamist Challenge: Nigeria's Boko Haram Crisis Explained', *African Security Review* (June, 2010) Vol. 19(2).

Onuoha, Freedom C., 'Why do Youth Join Boko Haram', *United States Institute of Peace Special Report* (June, 2014) No. 345.

Orji, Uchenna Jerome, 'A Review of the Special Duties of Banks under the Nigerian Money Laundering Act', *Journal of International Banking Law and Regulation* (2011) Vol. 26, (6).

Oyebode, Akin, 'Legal Responses to the Boko Haram Challenge: An Assessment of Nigeria's Terrorism (Prevention) Act 2011', *Forum on Public Policy* (2012).

Sampson, Isaac T. and Onuoha, Freedom C., 'Forcing the Horse to Drink or Making it Realize its Thirst? : Understanding the Enactment of Anti-Terrorism Legislation (ATL) in Nigeria', *Perspectives on Terrorism* (2011) Vol. 5(3-4).

Walker, Andrew, 'What is Boko Haram?', *United States Institute of Peace Special Report* (June, 2012)

Zenn, Jacob, 'Boko Haram and the Kidnapping of the Chibok School Girls', *CTC Sentinel* (May, 2014) Vol.7 (5).

Reports/Thesis

Amnesty International, *Nigeria: Trapped in the Cycle of Violence* (Amnesty international: London, United Kingdom, 2012).

Doukhan, David, *Defeating Boko Haram: The Realty on the Ground is Deceptive* (International Institute for Counter Terrorism: Israel, 26 November, 2015).

Human Rights Watch, *Those Terrible Weeks in their Camp – Boko Haram Violence Against Women and Girls in Northeast Nigeria* (Human Rights Watch: United States of America, 2014).

Human Rights Watch, *Those Terrible Weeks in their Camp: Boko Haram Violence against Women and Girls in Northeast Nigeria* (Human Rights Watch: United States, 2014).

Nigerian Institute of Advanced Legal Studies, *Dealing with the Past: Justice, Reconciliation and Healing in the North East of Nigeria* (Nigeria Stability and Reconciliation Programme: Abuja, Nigeria, 2017).

Rock, Jason L., *The funding of Boko Haram and Nigeria's Actions to Stop It* (A Master of Science submitted to the United States Naval Postgraduate School (California: December, 2016).

United Nations Development Programme (UNDP), *Human Development Report 2015* (UNDP: New York, USA, 2015).

UNDP, *Human Development Report 2016: Human Development for Everyone* (UNDP: New York, USA, 2016).

Articles in Newspapers/Online Sources

Adeyeye, Tobi, 'Northern Groups Protest Ban on Boko Haram, Ansaru', *The Herald* (6 June, 2013) available at <http://www.hearld.ng/northern-groups-protest-ban-on-boko-haram-ansaru/>.

AFP, 'Policemen Accused of Killing Boko Haram Founder Reinstated', *The Guardian* (19 February, 2018) available at <https://m.guardian.ng/news/policemen-accused-of-killing-boko-haram-founder-reinstated/>.

Ali Adoji, 'Boko Haram Robs Bank, Kills 4 in Maiduguri', *Daily Post* (31 March, 2012) available at <http://dailypost.ng/2012/03/31/boko-haram-robs-bank-kills-4-in-maiduguri/>.

Aljazeera, 'Nigeria Killings Caught on Video', (10 February, 2010), available at <https://www.aljazeera.com/news/africa/2010/02/20102505798741.html>.

Azu, John Chuks, 'Over 3000 Boko Haram Cases Stall in Courts', *Daily Trust* (10 September, 2017), available at <https://www.dailytrust.com.ng/over-3-000-boko-haram-case-stall-in-courts.html>.

BBC 'Boko Haram Declares 'Islamic State' in Northern Nigeria', *BBC News* (25 August, 2014), available at <http://www.bbc.com/news/world-africa-28925484>.

BBC, 'Nigeria Boko Haram Militants Technically Defeated – Buhari', *BBC News* (24 December, 2015) available at <https://www.bbc.com/news/world-africa-35173618>.

BBC, 'Nigeria Policemen in Court Trial for Boko Haram Killing', *BBC News* (13 July, 2011) available at <http://www.bbc.com/news/world-africa-14136185>.

BBC, 'Nigeria's Boko Haram Rejects Jonathan's Amnesty Idea', *BBC News* (11 April, 2013) available at <http://www.bbc.com/news/world-africa-22105476>.

BBC, 'Nigerians Living in Poverty Rise to Nearly 61 Percent', *BBC News* (13 February, 2012), available at <http://www.bbc.com/news/world-africa-17015873>.

Burke, Jason, 'Secret Trials of Thousands of Boko Haram Suspects to Start in Nigeria', *The Guardian* (9 October, 2017), available at <https://www.theguardian.com/world/2017/oct/09/nigeria-begin-secret-trials-thousands-boko-haram-suspects>.

Campbell, John, 'Boko Haram is Back in the Media Spotlight, but it was Never Really Gone', *Council on Foreign Relations* (20 September, 2019), available at <https://www.cfr.org/blog/boko-haram-back-mdeias-spotlight-it-was-never-really-gone>.

Council on Foreign Relations, *Global Conflict Tracker: Boko Haram in Nigeria* (31 October, 2019), available at <https://www.cfr.org/interactive/global-conflict-tracker/conflict/boko-haram-nigeria>.

Counter Extremism Project, *Boko Haram* (2019), available at <https://www.counterextremism.com/threat/boko-haram>.

Counter Terrorism Guide, 'Boko Haram', available at <https://www.dni.gov/nctc/groups/boko_haram.html>.

Egbas, Jude, 'Security Challenge: How Nigerian Army is Taking over the Job of the Police', Pulse Nigeria (4 October, 2018), available at <https://www.pulse.ng/news/local/how-nigerian-army-is-taking-over-job-of-the-police-id8205276.html>.

Ekott, Ini, 'Government White Paper Indicts Prominent Politicians for Creating Boko Haram', *Premium Times* (28 April, 2013), available at <https://www.premiumtimes.ng.com/news/131/694-government-white-paper-indicts-prominent-politicians-for-creating-boko-haram.htm>.

Farourk Chothia, 'Who are Nigeria's Boko Haram?', *BBC News* (26 August, 2011), available at <http://www.bbc.co.uk/new/world-africa-13809501>.

Gaffey, Conor, 'Cost of Terrorism: Boko-Haram has Destroyed $5.2 Billion Worth of Property in just One State in Nigeria', *Newsweek* (8 August, 2017) available at <http://www.newsweek.com/cost-terrorism-boko-haram-nigeria-64854>.

Giles, Christopher, 'Nigerian Elections: Has Boko Haram Been Defeated?', *BBC News* (8 February, 2019), available at <https://www.bbc.com/news/world-africa-47047399>.

Godwin, Ameh Comrade, 'North Kicks against FG's Decision to Ban Boko Haram, Ansaru', *Daily Post* (6 June, 2013), available at <http://dailypost.ng/2013/06/06/north-kicks-against-fgs-decision-to-ban-boko-haram-ansaru/>.

Human Rights Watch, 'Nigeria: Prosecute Killings by Security Forces', (26 November, 2009/11/26/Nigeria-prosecute-killings-security-forces>.

Ibrahim, Abubakar Adam, 'Boko Kills 1,100 Since Being Technically Defeated', *Daily Trust*, (3 December, 2017), available at <https://www.dailytrustcom.ng/boko-haram-kills-1-100-since-being-technically-defeated-html>.

Komolafe, Kayode, 'Boko Haram: A Crisis in Search of Strategy', *Thisday* (25 January, 2012).

Marama, Ndahi, 'Boko Insurgents Have Been Defeated – Buratai', *Vanguard* (8 January, 2018), available at <https://www.vanguard.ngr.com/2018/01/boko-haram-insurgents-defeated-buratai>.

Mutum, Roland, and Azu, John Chuks, 'Police Reinstate Officers Acquitted of Killing Boko Haram Leader', *Daily Trust* (19 February, 2018), available at <https://www.dailytrust.com.ng/police-reinstate-officers-acquitted-of-killing-Boko-haram-leader.html>.

Nnochiri, Ikechukwu, 'FG Okays Trial of 1,600 Alleged Boko Haram Terrorists, Frees 220 Suspects', *Vanguard* (24 September, 2017), available at <https://www.vanguardngr.com/2017/09/fg-okays-trial-1600-alleged-boko-haram-terrists-frees-220-suspects/>.

Ojeifo, Sufuyan, and Nzechi, Onwuka, 'Terror Blacklist: US Gives Nigeria Four Conditions', *Thisday* (12 February, 2010), available at <http://www.thisdayonline.com/nview.php?id= 166347>.

Ola-David, Tolulope, 'Is Boko Haram re-creating a Caliphate in Africa?', *Global Risks Insights* (4 September, 2015), available at <https//www.globalriskinsights.com/2015/09/is-boko-haram-re-creating-a-caliphate-in-africa/>.

Opejobi, Seun, 'Buhari Claims Boko Haram Technically Defeated', *Daily Post* (6 February, 2016) available at <http://dailypost.ng/2016/02/06/buhari-claims-boko-haram-technically-defeated/>.

Page, Matthew T., 'Nigeria Struggles With Sector Reform', Chatham House Experts Comments (2 April, 2019), available at <https://www.chathamhouse.org/expert/comment/nigeria-security-sector-reform>.

Reuters, 'Gunmen Free 175 Inmates in Nigeria Prison Break', *The Telegraph* (30 June, 2013) available at <https://www.telegraph.co.uk/news/worldnews/africaandindianocean/nigeria/1015154.6/ Gunmen-free-175-inmates-in-Nigeria-prison- break.html>.

Smith, David, 'More than 700 Inmates Escape during Attack on Nigerian Prison', *The Guardian* (8 September, 2010) available at <https://www.theguardian.com/world/2010/Sep/08/muslim-extremists-escape-nigeria-prison>.

Taiwo, Shakirudeen, 'Technically Defeated Boko Haram Carried out 135 Terror Attacks in 2017 – UN Envoy", *Business Insider* (12 January, 2018), available at <http://www.pulse.ng/bi/politics/technically-defeated-boko-haram-carried-out-135-attacks-id7837805.html>.

United Nations, 'Sanctions Committee Adds Boko Haram to its Sanctions List', *United Nations Press Release* (22 May, 2014) SC/11410, available at <https://www.un.org/press/en/2014/sc11410_do.htm>.

United States Department of State, 'Foreign Terrorist Organizations', available at <https://www.state.gov/j/ct/rls/other/des/123085.htm>.

Walker, Andrew, 'Why Nigeria has not Defeated Boko Haram', *BBC News* (14 May, 2014) available at <https://www.bbc.com/news/world-africa-27396702>.

Legislations and Policy Instruments

Administration of Criminal Justice Act.

Constitution of the Federal Republic of Nigeria (1999).

Economic and Financial Crimes Commission (Establishment) Act 2004.

Federal Republic of Nigeria, *National Security Strategy* (November, 2014).

Federal Republic of Nigeria, *Policy Framework and National Action Plan for Preventing and Countering Violent Extremism* (August, 2017).

Money Laundering Prohibition Act 2011.

Nigeria National Counter Terrorism Strategy (Office of the National Security Adviser, Abuja, August, 2016).

Office of the National Security Adviser, *The National Counter Terrorism Strategy (Revised)* (2016).

Terrorism (Prevention) Act, No.10 (2011).

Terrorism (Prevention) (Amendment) Act 2013, *Official Gazette of the Federal Republic of Nigeria* (22 April, 2013) Vol. 100, No.25, Government Notice, 70.

Terrorism (Prevention) (Proscription Order) Notice, 2013, *Official Gazette of the Federal Republic of Nigeria*, (24 May, 2013) Vol. 100, No. 34.

This Page Intentionally Left Blank

PUBLISHING PRINCIPLES

Articles sent to the ***Defence Against Terrorism Review*** must not be published elsewhere or must not have been sent to another publication in order to be published. Once the articles are submitted to DATR, the authors must acknowledge that they cannot submit their articles to other publications unless the total rejection of concerned articles by the Editor or the Endorsement Committee (EC).

The authors who try to submit their already published (even electronically) articles to DATR will not be accepted to submit their articles again and will be forbidden to participate any future activity conducted by COE-DAT.

A. GENERAL PRINCIPLES

1. Language of publication is English. The texts submitted must be clear and understandable, and be in line with scientific/academic criteria in terms of language, expression and citation.

2. The texts submitted to be published must be between 4000 and 12000 words including the abstract and bibliography.

3. The texts must be submitted together with an abstract no longer than 300 words at the beginning of the paper and with five keywords after the abstract.

4. The name of the author must be placed in the first footnote, with his/her title, place of duty and e-mail address. Footnotes for other explanations must be provided both in the text and down the page in numbers.

5. The type character must be Arial, "11 type size", line spacing "1,5 nk", footnotes in "9 type size" and with "single" line spacing.

General Contents

The following are general stylistic conventions used by COE-DAT:

1. Writing must be scholarly in nature and not overly conversational. Do not use "I" or "we" but "the author" or the "authors."

2. Do not use contractions except in quotes.

3. Except in quotes, do not underline or bold text to emphasize it but instead use word order for emphasis. To highlight a term, show the key words in single mark ('aerospace').

4. Use italic font for foreign phrases and names of court cases.

5. For dates, use – date month year format (10 March 2011) – not numbers (10/03/11). In footnotes, dates of the sources may follow the format used in the source.

6. There should be only one space between the period at the end of a sentence and the beginning of the next sentence.

7. Acronyms should be defined when first used with the full name in parentheses after the acronym; acronyms in foreign languages should have the name in the foreign first in parentheses, followed by the English translation. If an acronym has been defined once in the text of the article, it is unnecessary to spell it out again either in text or footnotes.

8. Numbers less than twenty or less should be spelled out; numbers 21 and above should be left in numbers.

9. Values in currency should be quoted in the actual currency followed by the amount in dollars (USD) or euros (€) in parentheses.

10. While making quotations;

a. If the part taken from the source is 4 lines and less than 4 lines, quotation marks ("...sentence...") can be used.

b. If the part taken from the source is more than 4 lines, it must be given with extra indentations.

- In addition, the writer of the article must avoid excessive use of each source, in particular from their own previous writings.

B. PRINCIPLES AS TO PAGE LAYOUT

Formatting: Double-spaced with standard page margins. The text and all headings should be left justified. Set language as American English. The publisher employed by COE-DAT uses a particular document formatting that will be applied by the editors.

C. PRINCIPLES AS TO REFERENCES AND CITATIONS

Citations shall be given down the pages in numbers in Defence Against Terrorism Review and references shall not be presented in the text (e.g. Waltz, 2009: 101.).

Full identity of the resources cited shall be given; any resource not actually cite shall not be presented in the bibliography.

Format for footnote citations;

1. For Books

a. Books with Single Author:

Name and surname of the author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s). For example;

Joseph Needham, *Science and Civilization in China,* (Vol. 5, Cambridge Univ. Pres, 1954), p.7.

Joseph Needham, *Science in Traditional China* (Harvard Univ. Pres, 1981), p. 37.

b. Books with Two or Three Authors:

Name and surname of the first author, name and surname of the second author, name and surname of the third author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s). For instance;

Joseph S. Nye Jr. and David A. Welch, *Understanding Global Conflict and Cooperation*, (Pearson Publication, 2011), p. 280.

c. Books with More Than Three Authors:

Name and surname of the first author et. al., *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s). For example;

Luis Benton et. al., *Informal Economy,* (The John Hopkins University Press, 1989), pp. 47-59.

d. Books with Name of Author or Editor Non-Specified:

Redefining Security (Praeger Publication, 1998), p. 81.

2. For Articles

Name and surname of the author (for all authors if two or three, if more than three authors just for the first author and et. al.), "name of the article" (translator if any), *name of periodical in which it is published*, volume number (issue) (publication year), pages in journal, cited page number.

a. Articles with One Author:

Barry Buzan, "New Patterns of Global Security in the Twenty-First Century," *International Affairs* 67(3) (1991), pp. 431-451, p. 442.

b. Articles in Compilation Books:

Barry Buzan, "Is International Security Possible?", in *New Thinking About Strategy and International Security* (Ken Botth and Don Kaufman, eds, Harper Collins, 1991), pp. 31-55, p. 42.

c. Articles from Daily Newspapers:

Yossi Melman, "Computer Virus in Iran Actually Targeted Larger Nuclear Facility", *Haaretz* (22 September 2011), p. 7.

"Tehran's nuclear ambitions", *The Washington Post* (26 September 2009), p. 5.

3. For Theses

No italics shall be used for the titles of non-published theses. Name and surname of the author, "title of the thesis" (whether it has been published and academic degree of the thesis, institution and institute of the thesis, date of the thesis), page number. For instance;

Atasay Özdemir, "Approaches of the Effective Actors of the International System to Iran's Nuclear Programme" (Unpublished Doctoral Thesis, War College Strategic Researchs Institute, Istanbul, 2013), p. 22.

4. For Reports

a. Report with Author Specified

Tariq Khaitous, "Arab Reactions to a Nuclear Armed Iran" (Washington Institute for Near East Policy, Policy Focus 94, June 2009), p. 14.

b. Report with Author Non-Specified

Albania Country Report (T‹KA Publishing, 1995), p. 7.

c. Report prepared by an Institution, Firm or Institute

American Petroleum Institute, "Drilling and Production Practice Proceedings of the Spring Meeting" (Shell Development Company, 1956), p. 42.

d. For Internet Resources

If any of the above resources are available on the Internet, follow the citation above with "available at" with the full http address and the date accessed in paratheses.

e. Web Pages

"The World Factbook-Turkey," Central Intelligence Agency, available at https://www.cia.gov/library/publications/the-world-factbook/geos/tr.htm (accessed 25 February 2013).

"Dimona: Negev Nuclear Research Center," *Global Security*, available at http://www.globalsecurity.org/wmd/world/israel/dimona.htm (accessed 11 January 2010).

"Russia's National Security Strategy to 2020" (12 May 2009), *Rustrans*, available at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (accessed 02 May 2011).

5. Subsequent citations of the same source:

a. If the citation is to the footnote directly before, use "Ibid" – if the page or paragraph changes, you can add the new information, as in "Ibid, p. 48" or "Ibid, para. 68".

b. If the source is earlier than the previous one, use the author's last name (if there is one), followed by the name of the article, followed by the new page or paragraphe number. For example;
Buzan, "Is International Security Possible?", p. 48.

D. PRINCIPLES TO ABIDE BY IN USING OF DOCUMENTS, TABLES, FIGURES AND GRAPHICS

1. Attachments (documents), shall be presented at the end of the text and down below shall be a brief information as to the content of the document and proper citation in line with the relevant criteria.

2. Other attachments (Table, Figure, and Graphics) shall be presented as Additional Table: 1, Additional Graphic: 3 and Additional Figure: 7. If indicators other than the text are too many in number; attachments shall be presented after the References.

a. References to these attachments in the text shall absolutely be made as Additional Table: 1, Additional Graphic: 3 or Additional Figure: 7.

b. If citation has been made for table, figure, graphic or picture, the source shall absolutely be indicated.

3. The names of the tables within the text shall be written on the top of the table and these tables shall be cited in the footnote according the publication type from which it was cited.

4. The names of the figures, graphics and maps within the text shall be written at the bottom of the figures, graphics and maps and these figures, graphics and maps shall be citied in the footnote according the publication type from which it was cited.

E. PRINCIPLES TO ABIDE BY IN BIBLIOGRAPHY

1. Just like giving citations but this time surname of the author shall be at the beginning.
2. Resources shall be sorted alphabetically from A to Z.
3. Page numbers shall not be indicated.

COE-DAT