Vol.16 • 2022

ISSN. 1307 - 9190

Defence Against Terrorism Review

E-DATR

COE-DAT
Centre of Excellence Defence Against Terrorism

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

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

E-DATR is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT). The information and views expressed in this e-journal are solely those of the lecturers and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturers are affiliated.

To cite an article in this e-journal, use the template illustrated below:
Surname, First letter of Name with a full stop (2022), The Headline of Article, Defence Against Terrorism Review (E-DATR), Vol.16., p. … - … .

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

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

Bu elektronik dergiden alıntı yapmak için aşağıdaki şablonu kullanınız:
Soyadı, Adın İlk Harfi ile sonuna nokta (2022), Makalenin İngilizce Adı, Defence Against Terrorism Review (E-DATR), Vol.16., p. … - … .

Defence Against Terrorism Review
E-DATR

Vol. 16, 2022

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), which is composed of representatives from 9 nations, focuses on providing key decision-makers with realistic solutions to terrorism and Counter-Terrorism (CT) challenges. COE-DAT fosters the sharing of expertise, information and best practices in countering terrorism, for allies within NATO and for partner nations. As an integral part of these efforts, COE-DAT proudly presents 16th Volume of DATR which features four articles on a wide range of aspects of terrorism.

The current issue begins with an article by Director of COE-DAT Col. Oğuzhan Pehlivan titled *"COE-DAT Contributions to Counter Terrorism on the 70th Anniversary of Türkiye's Membership to NATO".* In this article, Pehlivan describes that as a strong partner ally of NATO, Türkiye has always been on the front lines of struggle for defence against terrorism. COE-DAT, which was inaugurated in 2005, is one of the main contributors to this endeavour. Having discussed the Global Counter-Terrorism Strategy, he handles important issues which COE-DAT focuses, such as the Nuclear Terrorism, Terrorism Financing and Cryptocurrencies, Gender and Women in Terrorism, Capacity Building (CB) in Counter Terrorism (CT), Technology and New Trends, Cyber Domain and Security, Media and Terrorism, Pandemics and Bio-Terrorism. The conclusion of this article focuses on the importance of COE-DAT as one of the NATO accredited Centre of Excellence Centers. Col. Pehlivan concludes that COE-DAT is still effective in counter terrorism concept and doctrine development, as capacity builder in the Education and Training pillar, and Department Head (DH) of CT in global programming. The cumulative expertise and knowledge, which has been collected since inauguration, has been progressing each day with the contributions of sponsoring nations of the centre.

The second article of this issue by Captain Özgür Gürbüz focuses on the Recruitment Process of Terrorist Organizations by the help of the Internet. In his article entitled "*Internet-Supported Recruitment of Terrorist Organizations: An Analysis of the Early Stages of the Recruitment Process and Countermeasures to Prevent Terrorist Recruitment*", Gürbüz examines how terrorist organizations perform their internet-supported recruitment process, what tools they use, and how the authorities can combat the recruitment of terrorist organizations by intervening in the early stages of the process. After analyzing the relationship between terrorism, the media, and the internet from a historical perspective, he examines the internet-supported recruitment process with its stages and the internet-based tools used in the process. The last part analyzes how the human resources of terrorism can be rendered dysfunctional with countermeasures and practices developed at the initial stage of the internet-supported recruitment process. This study essentially aims to reveal that the human resources of terrorist organizations can be weakened much more effectively with the national and international countermeasures and practices taken at the very beginning of the internet-supported recruitment process. Gürbüz concludes that it is hard to fight the internet-supported recruitment of terrorist organizations only with hard countermeasures. He recommends that digital resilience against terrorism should be established, and the internet literacy of individuals should be improved to render the recruitment efforts of terrorist organizations dysfunctional.

Tolga Ökten, from Turkish National Defence University, discusses the concept of lone actor, which has gained popularity again recently in the third article of this issue titled "*Lone Actor Attacks and Organizational Connection: An Analysis of al Qaeda and Daesh Inspired Attacks in the European Union Zone*". In this article, Ökten argues that lone actors have some distinct characteristics and that is why they are a real threat to European security. These features are theorized within the framework of the organizational connection variable, and the differences between lone actor and other organized attacks are examined. Having explained the Strategic Logic of Lone Actor Attacks, the author analyses the attacks in terms of Mental Health, Lone Actor-Crime Nexus, Legal Status, Targets and Tactics. Ökten argues that al Qaeda and Daesh inspired lone actors are real and they constitute a significant threat to global security. Lone actor attacks are executed in isolation and that is why they can be classified separately from other attackers like FTFs and cell formations. According to both statistical and descriptive analysis of these attacks, Ökten concludes that lone actor attacks are used as a conscious strategic choice by al Qaeda and Daesh leadership because of their unique characteristics. As a proven unconventional method, in the future, lone actor attacks will most likely continue to be an important strategical choice for terrorist organizations.

In the last article of this issue entitled "*Children Recruiting and Exploiting by Terrorist Groups*", Zehra Eroğlu Can addresses the importance of recruiting children by terrorist groups. Can examines the reasons and the methods used by terrorists to recruit children. The author describes the methods of terrorist groups to recruit children as: forcible recruitment, economic enticement, transnational recruitment, use of schools (education), propaganda and online recruitment. He argues that terrorist groups prefer recruiting children due to visibility and propaganda, economic considerations and effectiveness, easy control and tactical advantages. A large number of children are being trafficked by terrorist and violent extremist groups. The children in these groups face to extreme violence and as a result they could easily have physical and mental harm, so rehabilitation and reintegration programs are main milestones in their new life. The author also recommends that governments ought to support transnational and multidisciplinary cooperation to create and carry out programs taking care of instances of children having been presented to terrorist groups. Sustained activities of the reintegration network would involve four components of de-radicalization, re-education, reintegration and community outreach jurisdictions as well.

As DATR team, we would like to thank all authors for the contributions they have made to this issue and the reviewers for their thoughtful comments and efforts towards improving our manuscript. DATR always welcomes and encourages contributions from experts, civil and military officers as well as academics to send us their comments, suggestions and rewarding work on defence against terrorism.

Sincerely yours,

Uğur Güngör

Editor-in-Chief

E-DATR, 2022; 16 : 7-34
ISSN 1307 - 9190

COE-DAT Contributions to Counter Terrorism on the 70th Anniversary of Türkiye's Inauguration to NATO

Oğuzhan Pehlivan[1]

Abstract: *After the Second World War, to secure peace in Europe and prevent further conflicts, North Atlantic Alliance Organization (NATO) was established. The Alliance's founding treaty was first signed in Washington in 1949 by a dozen European and North American countries. It dedicates the Allies to a more peaceful, libertarian and non-conflict environment.*[2] *NATO was largely dormant until the Korean War, especially in its military structure. During this war in 1952, Türkiye also became one of the new allies of NATO. Türkiye, which has been a member of NATO for 70 years, is the eighth largest contributor to the common fund, and has the second largest army in NATO. As a strong partner of NATO, Türkiye has always been on the front lines of the struggle for defence against terrorism. Centre of Excellence Defence Against Terrorism (COE-DAT), which was inaugurated in 2005, is one of the main contributors to this endeavour. From the moment of its foundation, COE-DAT, as an Education & Training (E&T) Facility, think-tank, and Department Head (DH) of Counter-Terrorism*

1 PhD, Director of Centre of Excellence-Defence Against Terrorism (COE-DAT), ORCID: 0000-0002-6779-4699, ozipehlivan@yahoo.com.

- The information and views expressed in this article are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.
- The author appreciate the efforts of Maj. Yahya BOLAT, Ms. Müge MEMİŞOĞLU, Ms. Özge ERKAN, Ms, Hülya KAYA and Ms. Aslıhan SEVİM , who are staff of COE-DAT, on collecting data and overview of COE-DAT products.

2 https://www.nato.int/wearenato/why-was-nato-founded.html (Accessed May 15, 2022).

(CT) in NATO's Global Programming, has published 28 activity reports, 21 newsletters, 16 journals, 28 books, and 14 research reports. COE-DAT has conducted 35 Mobile Education events in 21 different countries, and as of today has executed 133 courses. COE-DAT is additionally appointed as the DH for Alliance CT E&T by the Supreme Allied Commander Transformation (SACT), and as such is tasked to coordinate, synchronize and de-conflict the growing quantity of NATO CT E&T events in order to provide training that is "efficient, effective and affordable" on behalf of Alliance members. COE-DAT continues today to present recommendations and suggestions for key decision makers at the strategic level.

Key Words: *COE-DAT, Terrorism, Countering Terrorism, Defence Against Terrorism.*

1. Introduction

There have been international security initiatives created to prevent conflicts and support peace since the Delian League, which was founded in 478 BC. The North Atlantic Treaty Organization (NATO), which aims to promote democratic values, enables members to consult and cooperate on defence, commits to the peaceful resolution of disputes, and uses military force in order to stabilize the situation if all these attempts fail, is one of these establishments.[3]

NATO was inaugurated in order to ensure security for the Western Bloc by using power if necessary, according to the international relations theory of realism. During the Cold War, NATO provided a collective defence against the Warsaw Pact, and maintained its importance. The fall of Berlin Wall was the harbinger of the end of Cold War and declared a new age. Some scholars at that time thought that NATO also came to an end[4]. However; globalization, the rising power of Russia and China, and the presence of Weapons of Mass Destruction (WMD) were still threats to the NATO member countries in the beginning of the millennium. The countries, which see NATO's presence as vital for the future of their own security, made some efforts to retain the effectiveness of the organization.[5]

---

3 https://www.nato.int/nato-welcome/index.html (Accessed April 18, 2022).

4 Medcalf J. (2005). NATO: Beginners Guides. Oneworld Publications, Oxford.

5 Şahin, G. (2017). Küresel Güvenliğin Dönüşümü; NATO Bağlamında Kavramsal, Tarihsel ve Teorik Bir Analiz. *Savunma Bilimleri Dergisi*, *16*(2), 59-81.

Besides these developments, NATO, by easing collaboration between states and international organizations on security issues, by intervening in crisis and conflicts all over the world, and by providing a legal base for humanitarian aid and peace keeping, developed itself outside the field that it was originally created for.[6]

While there were some discussions about the necessity of NATO in academic literature, Türkiye strongly defends the soul of NATO in every platform. The recent developments occurring in Ukraine show the importance of Türkiye once again. There are still some hostilities between states of world, and NATO, as a security provider alliance, enhances its capability to negotiate and remains a deterrence and defence instrument for the unintentional or deliberate use of force.

Global terrorism has been one of the two primary security threats recognized by NATO since the 9/11 attacks in 2001. Türkiye, when it is compared with other NATO member states, is deemed to be most affected by terrorism according to the Global Terrorism Index (GTI) 2021, which measures incidents, fatalities, injuries and property damage impacts as shown in Table 1.[7]

Table 1. GTI Scores of NATO members

Rank	Country	GTI Score	Rank	Country	GTI Score
1	Turkey	5.651	16	Denmark	0.291
2	United States of America	4.961	17	Albania	0
3	Greece	4.849	18	Bulgaria	0
4	United Kingdom	4.77	19	Croatia	0
5	Germany	4.729	20	Estonia	0
6	France	4.562	21	Hungary	0
7	Canada	3.882	22	Iceland	0
8	Italy	3.687	23	Latvia	0
9	Spain	2.861	24	Macedonia (FYR)	0
10	Netherlands	2.077	25	Montenegro	0
11	Belgium	1.745	26	Poland	0
12	Norway	1.109	27	Portugal	0
13	Romania	1.06	28	Slovakia	0
14	Lithuania	0.827	29	Slovenia	0
15	Czech Republic	0.291	30	Luxembourg	No data

6 For further information, see NATO Key events in https://www.nato.int/nato-welcome/index.html.

7 https://www.visionofhumanity.org/maps/global-terrorism-index/#/ (Accessed April 18, 2022)

Türkiye, which has both enormous experience with and expertise on terrorism, declared the intention to found a Centre of Excellence in 2003. As a result of this endeavour, the Centre of Excellence Defence Against Terrorism (COE-DAT) was officially inaugurated in 2005. As only the second COE that achieved accreditation from NATO, COE-DAT received International Military Organization status in 2006 and has successfully conducted courses, seminars, workshops, conferences, Mobile Education Teams (METs) and other projects for NATO and partner nations all over the world ever since.

COE-DAT is a hub for counter-terrorism expertise and interacting with universities, think tanks, researchers, international organizations, global partners, and other COEs. As a result of this fruitful collaboration, COE-DAT has published 28 activity reports, 21 newsletters, 16 journals, 28 books, and 14 research reports – 107 hardcopy products in total, as shown in Figure 1. COE-DAT has conducted 35 Mobile Education events in 21 different countries, and to date has executed 133 courses. COE-DAT is additionally appointed as the DH for Alliance CT E&T by the Supreme Allied Commander Transformation (SACT), and as such is tasked to coordinate, synchronize and de-conflict the growing quantity of NATO CT E&T events in order to provide training that is "efficient, effective and affordable" on behalf of Alliance members. COE-DAT continues today to present recommendations and suggestions for key decision makers at the strategic level.

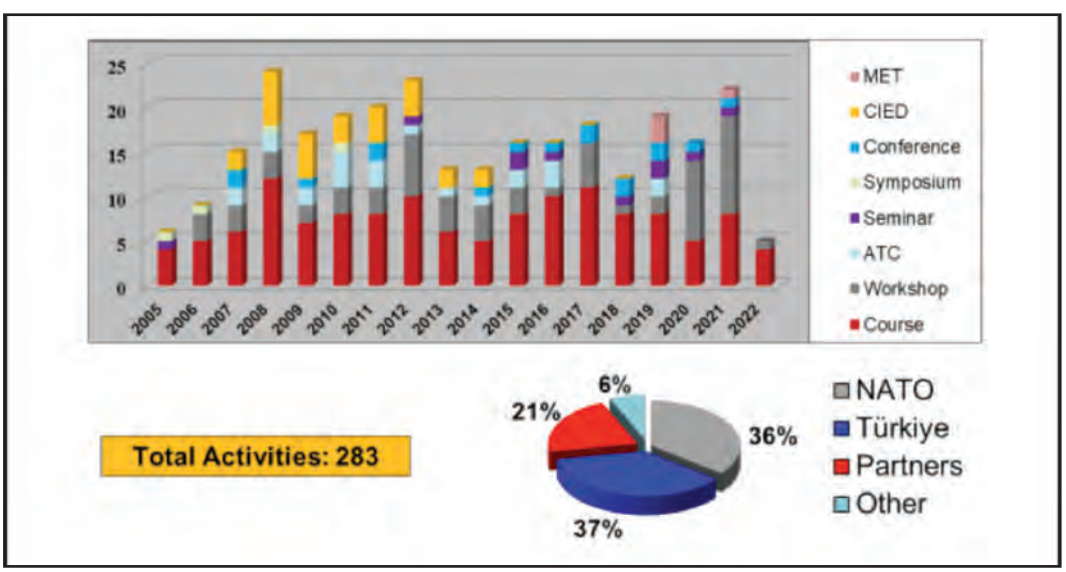


Figure 1. The Products of COE-DAT between 2005-2022.

Until 2010, COE-DAT publishing efforts focused primarily on activity reports and books. With the exception of 2018 and 2021, the Centre also published the *Defence Against Terrorsim Review* (DATR) every year as a periodical journal. Since 2014, COE-DAT has also dedicated significant effort to stand-alone research reports. In 2022, COE-DAT has seven research projects ongoing with great contribution to the counter terrorism (CT) discipline.

The aim of this article is to scrutinize the enormous value added by COE-DAT in CT, summarize the main key findings, and reveal the legitimacy and effectiveness of COE-DAT's products. This article also creates an opportunity for COE-DAT to link the outcomes of projects and other products back to the Centre's E&T department, as the findings feed the construction of courses, WSs, seminars, and METs. As it was stated by Mustafa Kemal ATATÜRK, the founder of Türkiye Republic, the author's basic intention is to be faithful to the scholars of COE-DAT's products, otherwise "*If the writer does not remain faithful to the creator, the unchanging truth takes on a nature that will surprise humanity.*"[8]

2. From 2005 to 2022, CEO-DAT's Contributions and Food for Thought

2.1. Global Counter-Terrorism Strategy

Today, there is no single definition of terrorism; its meaning unfortunately changes according to its usage by states and international organizations. In Table 2, we can see that a recent study indicated widespread agreement on the inclusion of violence and political motivation as definitional elements of terrorism, but very little agreement on any other concept proposed.[9]

---

8 Çambel, Hasan Cemil (1939). Belleten, Türk Tarih Kurumu Yayınları, Cilt:3, Sayı:10, 272.

9 Schmid, A. P., Forest, J. J., & Lowe, T. (2021). Terrorism Studies. *Perspectives on Terrorism*, *15*(3), 142-152.

Table 2. The Definition of Terrorism (Schmid et. al, 2021: 143)

Rank	Definition	Percentage	Rank	Definition	Percentage
1	Violence or force as element of definition:	91.1	13	Coercion:	20
2	Political as element:	82.2	14	Propaganda:	20
3	Civilians, non-combatants as victims:	48.9	15	Random, indiscriminate character:	15.6
4	Targeted, target, emphasized	46.7	16	Symbolic character:	15.6
5	Threat, fear, or intimidation emphasized:	46.7	17	Government or state as victim:	15.6
6	Non-state group, movement or organization as perpetrator:	37.8	18	Criminal, illegal nature:	15.6
7	Emphasis on non-state individuals as perpetrators:	35.6	19	Psychological character emphasized:	15.6
8	Ideology, ideological	33.3	20	Method of combat, strategy, tactic:	11.1
9	Violence or force as element of definition:	28.9	21	Clandestine, covert nature:	11.1
10	State or sub-state actor as perpetrator included:	22.2	22	Anxiety-inspiring:	11.1
11	Deliberate, planned, calculated or organized action:	20	23	Economic harm emphasized	11.1
12	Extra-normal, in breach of accepted (moral or legal) rules:	20			

In order to construct a counter-terrorism strategy, the first step should be to define terrorism and counter-terrorism. This is the reason NATO wrote the MC0472/1 document ("Military Committee Concept for Counter-Terorism") in 2016[10]. In order to enhance the Alliance's prevention of, response to and resilience after acts of terrorism.COE-DAT contributed great effort to the preparation process of MC0472/1 by focusing on underlying principles and potential initiatives in relation to awareness, capabilities and engagement, as those concepts are defined by NATO's 2012 policy guidelines on counter-terorrism[11].

COE-DAT continues to undertake efforts and projects to define concepts and doctrine for defence against terrorism. To maintain a multi-domain perspective, COE-DAT has a wide range of networks, tries to provide both military and political points of view from different scientific disciplines, and leverages the results of those endeavours.

---

10 https://www.nato.int/nato_static_fl2014/assets/pdf/topics_pdf/20160905_160905-mc-concept-ct.pdf (Accessed April 20, 2022).

11 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/ct-policy-guidelines.pdf (Accessed April 20, 2022).

In 2018, Genna articulated in her DATR article that while all NATO Allies confirm that there is a need to emphasize the conditions that spread terrorism[12], countering violent extremism (CVE) and preventing violent extremism (PVE) are thought areas outside of the Alliance's mandate. However, NATO can contribute to these efforts and obtain added value.[13]

The Global Terrorism Index (2022) report mentioned that even though religiously motivated terrorism is dominant worldwide, politically motivated terrorism is also on the rise. According to this report,

> *Politically motivated terrorism has now overtaken religiously motivated terrorism, with the latter declining by 82 per cent in 2021. In the last five years, there have been five times more politically motivated terrorist attacks than religiously motivated attacks. There are now noticeable similarities between far-left and far-right extremist ideologies, with both targeting government and political figures. Since 2007, 17 per cent of terrorist attacks by these groups have targeted this category.*[14]

The author of this article has recommended that NATO deal with terrorism at its source, and while executing this fight against terrorism, extremism and radicalism also should be handled and examined together with terrorism.

2.2. Nuclear Terrorism

Nuclear terrorism includes four master types of terrorist activity. First, the robbery and usage of a pristine nuclear apparatus; second, the burglary or other acquisition of fissile material that should later be used to produce a nuclear weapon; third, assaults on reactors or other nuclear facilities; and last but not least, the usage of radiological material in order to produce a radiological dispersal device (RDD).[15] There is always possibility for terrorists to steal and use nuclear weapons, and it has been discussed in many states (like the US and others) before.[16]

---

12 "Brussels Summit Declaration" (2018), NATO, para 10, at https://www.nato.int/cps/en/natohq/official _texts_ 156624.htm 9 (Accessed April 20, 2022).

13 Genna, Federica (2018). "*NATO's Enhanced Role in Counter Terrorism*", Defence Against Terrorism Review, Vol. 10, pp. 9- 21.

14 https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web.pdf (Accessed April 20, 2022).

15 Cameron, G. (1999). Nuclear terrorism: A threat assessment for the 21st century. Springer.

16 Nuclear Terrorism: Frequently Asked Questions, Belfer Center for Science and International Affairs https://www.belfercenter.org/publication/nuclear-terrorism-faq (Accessed May 16, 2022).

Although at present there is no reliable proof that any terror organization or terrorist member have achieved in obtaining Category I special nuclear material (the multi-kilogram, critical-mass amounts of uranium 235, uranium 233, or plutonium required to make a nuclear weapon), the burglary of small amounts of fissile material can be seen as a possible option for them.[17]

NATO recognizes that the nexus of the proliferation of WMD and terrorism is a major threat to the security of the Alliance, as first stated in NATO's 1999 strategic concept. COE-DAT, with the collaboration of NATO Headquarters Emerging Security Challenges Division (ESCD), prepared a book called "Response to Nuclear and Radiological Terrorism", edited by Dan-Radu Voica and Mustafa Kibaroğlu. In this book, the authors made initial assessments of nuclear, radiological, and biological weapons, and explored future concepts in defence against terrorism as it applied to these threats. While NATO still considers nuclear weapons to be a deterrence instrument, especially against Russian aggression, nuclear *energy* seems to be one of the alternatives for reducing dependency on fissile material - furthermore, in view of climate change and global warming, nuclear energy makes sense for future feasible energy supply. In order to prevent the spread of WMD, strong multilateral collaboration and global network capability are required; optimizing multinational solutions for operational, communication and logistical response may also prevent the spread of WMD. To counter radiological/nuclear terrorist attacks effectively, it is essential to define standards for protecting weapons and materials as the first step to fill the gaps in Allied defences.[18]

Today, scholars continue to argue over the same issues. Volders (2021) articulated that a more organic organizational design is likely to benefit the effective implementation of a nuclear terrorism project.[19] Most of the countries' criminal systems still face considerable statutory shortcomings in enforcing its nuclear terrorism laws.[20] In the future, in order to prevent four faces of nuclear terrorism for securities as shown in Figure 2, neural and social networks incorporated with

[17] Matthew Bunn. Preventing a Nuclear 9/11 Archived 2014-03-01 at the Wayback Machine Issues in Science and Technology, Winter 2005, p. v.

[18] Voica, Dan-Radu & Kibaroğlu, M. (Ed.) (2010). Response to Nuclear and Radiological Terrorism, NATO Science for Peace and Security Series E.Human and Societal Dynamics, Vol.2, IOS Press BV, Netherlands.

[19] Volders, B. (2021). The Nuclear Terrorism Threat: An Organisational Approach. Routledge.

[20] Mishra, R. (2021). Nuclear Terrorism: Statutory Shortcomings and Prosecutorial Opportunities. International Law Studies, 97(1), 23.

system dynamics, using data mining systems through cloud computing technology, should be constructed to enable systematic research on cell phones against possible terrorist incidents.[21] The author suggests using big data and artificial intelligence (AI) to provide security and resilience.

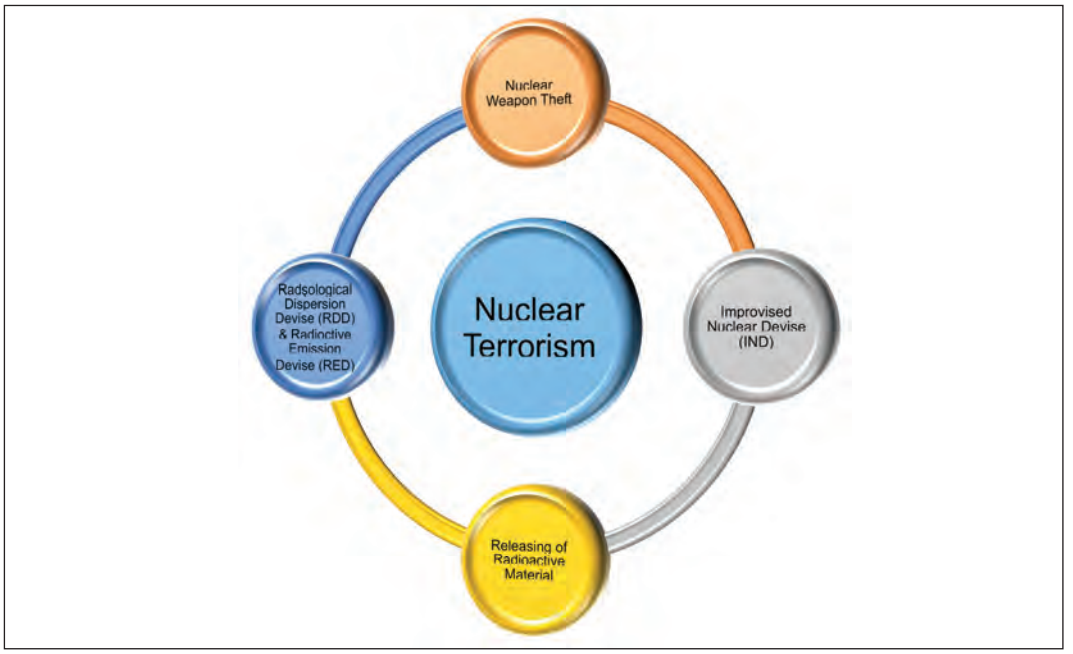


Figure 2. Four faces of nuclear terrorism for the securities (Jang et. al, 2021: 14)

2.3. Terrorism Financing and Cryptocurrencies

Scientific literature identifies Satoshi Nakamoto – who likely used a nickname and is allegedly a 36 year old Japanese man – as the inventor of cryptocurrency. There was no paper, no material subject, just thirty-one lines of internet code and an announcement on internet…and the birth of a new currency that operates beyond the monetary policies of states to facilitate an uncontrolled money flow.[22] To date, no government agency supports the use of cryptocurrencies. Furthermore, cryptocurrencies' ungoverned features attract ill-intended people, who might

[21] Jang, K. B., Baek, C. H., Kim, J. M., Baek, H. H., & Woo, T. H. (2021). Internet of Things (IoT) Based Modeling for Dynamic Security in Nuclear Systems with Data Mining Strategy. Journal of The Korea Internet of Things Society, 7(1), 9-19.

[22] Davis, J. (2011). The crypto-currency. *The New Yorker*, *87*.

use them for money laundering, narcotics, human trafficking, etc., and yet few national security organizations seem to recognize the threat. According to United States Treasury Department's Financial Crimes Enforcement Network (known as "FinCEN") Director Jennifer Shasky Calvery, while many in the financial community figured out this emerging payment system, many line analysts, investigators, and prosecutors in law enforcement did not.[23]

Brill and Keene (2014) noticed the hazard of terrorist usage of this new flow of currency and wrote an article with a headline "Cryptocurrencies: The Next Generation of Terrorist Financing?".[24] After explaining what cryptocurrency is, the authors explained how it works. Cryptocurrencies are created with the help of block chain technology by solving extremely difficult mathematical problems. The system is attractive to terrorists for ten primary reasons: First, cryptocurrencies offer *anonymity*. In this system, there are zero regulations requiring a user to produce an ID card. *Global reachability* is another attractive reason. Systemic *speed* allows rapid transfers of any amount. *Non-repudiation* provides no additional verification. *Low cost to use* makes the system more desirable. *Relative ease of use* mitigates technical difficulties. *Difficult for authorities to track transactions* is likely the most attractive part that draws attention of terrorists. *Potential upgrades to security and anonymity* cause law enforcement and anti-terrorism agencies to keep their eyes constantly open in order to enhance security. *Venue changes to make cooperation with governments* need collaboration of states and construction of unilateral understanding on terminology. At final stage, *complexity* makes the track of currency nearly impossible.

Even though some countries took steps to ban or limit cryptocurrency, the degree to which the use of virtual currencies can actually be controlled is questionable. The recommendations and further developments in these topics are listed below.

- *Update the Financial Action Task Force (FATF): FATF and the FATF-style regional bodies (FSRBs) have established 21 high-level principles to promote implementation worldwide since 2014; new improvements can be added to these regulations and institutions.*[25]

---

23 Ibid, p. 8.

24 Brill, A. & Keene, L. (2014). *"Cryptocurrencies: The Next Generation of Terrorist Financing?"*, Defence Against Terrorism Review, Vol. 6, No. 1, pp. 7- 30.

25 https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF%2025%20years.pdf (Accessed April 19, 2022).

- *Encourage the development of national (and international) self-regulatory organizations (SFO): The first crypto SROs organized outside the US, and the Virtual Commodity Association is considered an early attempt to form one inside the US. Later in 2014, a group of 10 financial and tech firms created the Association for Digital Asset Markets (ADAM), with 31 members and 5 partnering law firms.*[26]
- *Encourage an increased level of cooperation, knowledge-sharing and skills-sharing between the agencies and organizations responsible for anti-money laundering activities with those responsible for the interdiction of terrorist financing:* For instance, USA[27], EU[28], Africa[29] and Asia[30]are all making attempts to implement this kind of cooperation and capability sharing.
- *In the interdiction of terrorist funding, understand the broad range of laws that may be available for the prosecution of offenders:* UNODC began to discuss a draft document in 2007; their endeavours to update according to the new developments are ongoing.[31]
- *Maintain vigilance with regard to the evolution of virtual currencies:* FATF is still the main authorized establishment, and its recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.[32]

---

26 https://cointelegraph.com/news/self-regulatory-organizations-growing-alongside-new-u-s-crypto-regulation (Accessed April 20, 2022).

27 https://home.treasury.gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf (Accessed April 20, 2022).

28 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0371&rid=6 (Accessed April 20, 2022).

29 http://www.treasury.gov.za/publications/other/Mutual-Evaluation-Report-South-Africa.pdf (Accessed April 20, 2022).

30 https://asean.org/wp-content/uploads/2021/01/ASEAN-Documents-on-Combating-Transnational-Crime-and-Terrorism-1.pdf (Accessed April 20, 2022).

31 https://www.unodc.org/documents/terrorism/Handbook_on_Criminal_Justice_Responses_to_Terrorism_en.pdf (Accessed April 20, 2022).

32 https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (Accessed April 20, 2022).

2.4. Gender and Women in Terrorism

Perceptions of gender roles and the linkage to gender being a women's "issue" creates a "blind spot" in counter-terrorism efforts. Gender is more than women and men, as gender is a socially constructed phenomenon more than it is a biological one.[33] Gender is created by society on the axis of masculinity and femininity that are also impacted by "intersectional factors", such as race and religion. These structures aligned masculinity and men with violence, aggression, assertiveness, rationality, logic, while femininity and women are typically aligned with passivity, submission, emotions, frailty.

It is clear that women's participation in terrorism is not a new phenomenon. Since Vera Zasulich, who is the first woman to be tried in a court of law for terrorism in the late 1870s, there has been a steady rise in the number of recorded female terrorists. Women "have been active participants in 60% of armed groups" since the 1950s; they have historically helped found terror groups such as the Baader-Meinhof Gang and the Japanese Red Army, and will most likely form new groups in the future. In addition to this, the literature on women in terrorism has also been growing in recent years, and this increases make an enormous contribution toward a more holistic understanding of terrorism.[34]

On the surface, there may be no perceptible disparity between men and women when it comes to their motivations to radicalize. However, a deeper look allows us to see that some reasons cannot be the same. For example, sexual exploitation or sexual abuse is one of the significant reasons for women to become terrorists, but it rarely appears as a motivation for male radicalization. It is also important that this may be a cause before or conclusion after recruitment of women in terrorist groups.[35]

Western women who participate in terrorist organizations like Daesh may do so in pursuit of romanticism, adventure, empowerment, seeking the meaning of life; they may also arrive with problems like depression, self-destruction, troubled-childhood, and trauma.[36] Male motivations and mental health struggles may follow similar patterns, but the research is beginning to show that these manifestations differ in pattern and complexity.

There are many roles for women in terrorism. One of them is perpetrating terrorism. Women can also be survivors and victims of violence, and furthermore

[33] Wharton, A. S. (2009). *The sociology of gender: An introduction to theory and research*. John Wiley & Sons.

[34] Davis, J., West, L., & Amarasingam, A. (2021). Measuring Impact, Uncovering Bias? Citation Analysis of Literature on Women in Terrorism. *Perspectives on Terrorism*, *15*(2), 58-76.

[35] Yıldız, Seda Öz (2019). Women in Terrorism and Counterterrorism, Workshop Report of COE-DAT.

[36] Zizola, Anna (2019). Women in Terrorism and Counterterrorism, Workshop Report of COE-DAT.

women may actually fight for restrictions on women's rights. Preventing is the another role of women in terrorism. For example, Diyarbakır Mother can be enumerated as a good example for this role. Extremist groups use women and girls as a direct target. Sexual and gender based violence (SGV) is a intentional section of the ideology and strategic goals of many terrorist groups.[37]

Women can deliver precious contributions to different aspects of CT, including analysis, field work and policy development. Addtionally, women's empowerment and participation has played a crucial role in countering violent extremism; if women are capacitated socially and economically, the spread of violent extremism slows. There is always good reason to augment the participation of women in CT; NATO must insist its Allies and Partners engage female perspectives as much as they do male perspectives and analytically pursue gender integration across the operational and political spectrum.[38]

Disarmament, demobilization and reintegration (DDR) processes in post-conflict contexts is another important topic to be handled by states. DDR programmes must be gender-sensitive, working for both men and women. While reintegrating women, as with men, social support from the community is the key element. Within all stages of the DDR process, women must not be excluded.[39]

Although there are fewer female terrorists than male terrorists, it is clear that women have been involved in counter-terrorism for many years, in policing and intelligence roles. Additionally, when the recent scientific data is scrutinized thoroughly, there has been a rise in their participation in more direct operational roles, including police tactical intervention and military specialist operations.[40]

The current CT programs are generally not active less differentiated and less balanced in terms of gender focus. More complex planning should be needed. It is vital that all men and women working in the field of CT must have the same gender-sensitive training.

---

37 Women in Terrorism and Counterterrorism Workshop Report (2019). COE-DAT, https://www.tmmm.tsk.tr/publication/workshop_reports/08-WomenInTerrorismAndCounterterrorism.pdf (Accessed April 20, 2022).

38 Hutchinson, Clare (2019). "Enhancing women's participation in counterterrorism: NATO perspective". Women in Terrorism and Counterterrorism Workshop Report (2019). COE-DAT, https://www.tmmm.tsk.tr/publication/workshop_reports/08WomenInTerrorismAndCounterterrorism.pdf (Accessed April 20, 2022).

39 Davidian, Alison (2019). Women in Terrorism and Counterterrorism, Workshop Report of COE-DAT.

40 "Female Operators: Women in Special Forces"*, Jane's IHS Markit*, 2017, https://www.janes.com/images/assets /262/68262/Female_operators_Women_in_special_forces_edit.pdf (Accessed April 23, 2022).

2.5. Capacity Building (CB) in Counter Terrorism (CT)

According to the UN Office for Disaster Risk Reduction (UNISDR), capacity is "the combination of all the strengths, attributes and resources available within an organization, community or society to manage and reduce disaster risks and strengthen resilience".[41]

Capacity Building (CB) in any organizational body means focusing on staff development by conducting E&T programs to close the knowledge gaps of that organization or its personnel. CB is not a new area for NATO. After 9/11, NATO began transforming CB activities, countering not only traditional threats but also emerging threats in the new security environment like international terrorism.[42]

The 2002 Prague Summit is the milestone for inclusion of CT as a mission within CB. Furthermore, the Military Concept for Defense against Terrorism (MCDT), which was endorsed and agreed on by the Alliance leaders in 2002, also envisions the CT mission as contained within CB activities. The Military Committee Concept for CT (MCCT) in 2015 presented a framework, principles, and guidelines to provide for CT across the spectrum of NATO's activities. Construction of new organizational mechanisms, such as the COE-DAT and the ESCD also illustrates the amplification of the scope of CB. Besides these efforts, Partnership Training and Education Centers (PTECs) and NATO Schools have enlarged the capability of NATO in Education & Training (E&T).

Military exercises are, foremost, activities for enhancing and maintaining requested preparation levels and interoperability readiness. Until the 1990s, NATO maintained a dynamic exercise program to train forces in as many demanding scenarios as possible.[43] NATO leaders decided to increase their efforts on collective defence scenarios with an emphasis on the importance of military exercises in 2014, at the iWales Summit.[44]

COE-DAT has committed itself to that effort and has contributed greatly to CB of NATO in CT. Since the Centre's inauguration, COE-DAT has conducted 160 courses of 28 different types; and in these activities, 7561 participants and 1697

---

41 United Nations Office for Disaster Risk Reduction, "Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction", (2009), p.12

42 Sadık, Giray & Bekçi, Eda (2019). *"NATO Capacity Building in Counterterrorism and Transatlantic Cooperation",* Defence Against Terrorism Review, Vol. 11, pp. 45- 63.

43 NATO, "BI-SC Collective Training and Exercise Directive (CT&ED) 075-003", 2 October 2013.

44 Jens Stoltenberg, "The Secretary General's Annual Report 2017", NATO, at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_03/20180315_SG_AnnualReport_en.pdf (Accessed April 21, 2022).

lecturers (9258 personnel total) found a chance to come together, share knowledge, and augment the organizational capacity of CT efforts across the globe as shown in the Figure 3. To date, COE-DAT has executed "Defence Against Terrorism", "Efficient Crisis Management to Mitigate the Effects of Terrorist Activities", "Counter Terrorism/Attack the Network", "Terrorism and Media", "Defense Against Suicide Attack", "Terrorist Use of Cyberspace", "Critical Infrastructure Protection from Terrorist Attacks", and "Border Security, Refugees and CT" courses. Further, in addition to residential courses, COE-DAT made efforts to reach the unreachable by constructing and executing 27 Mobile Education Teams, educating 1384 people from Asia to Europe. These efforts on capacity building also strengthen bonds among and between NATO and partner nations.

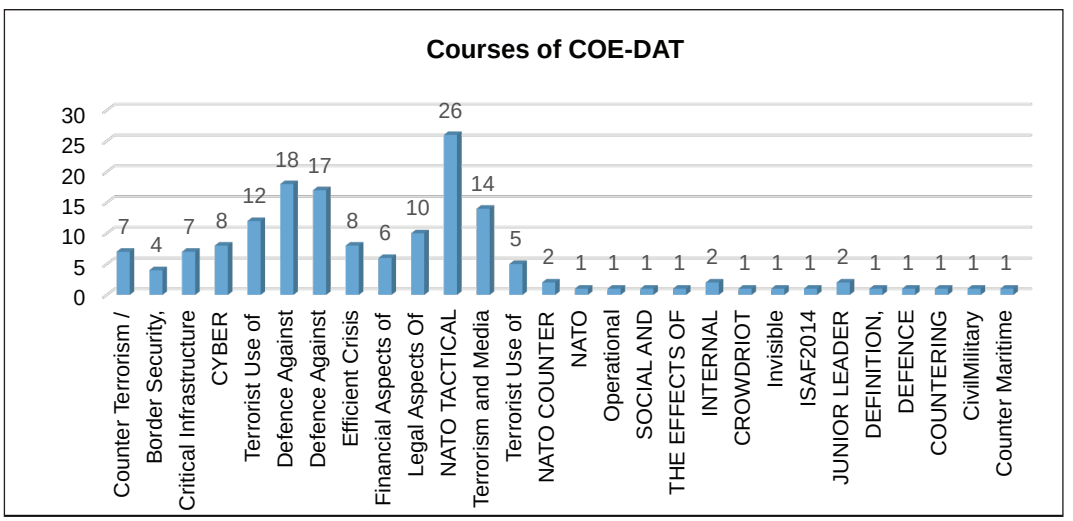


Figure 3. The courses of COE-DAT between 2005-2022.

The workshops, seminars and conferences are also added value for CB in CT. Every year, COE-DAT hosts a "Terrorism Experts Conference" and an "Executive Level Counter Terrorism Seminar", the Centre's flagship events. These activities bring together world-renowned expertise, knowledge, and academic literature in order to discuss current and future challenges in the CT domain. Last but not least, as a strategic-level think-tank establishment, COE-DAT continues to serve as a hub for academicians, scholars, military and civil staff, and encourages people from a wide selection of perpsectives to consider future trends in terrorism and strive to find solutions in the defense against terrorism. In an effort to push the level of courses from intermediate to advanced, COE-DAT continually seeks new research

projects, paving the way for participants of all COE-DAT events to understand, interpret and implement knowledge in novel situations.

2.6. Technology and New Trends

Terrorism is the struggle of mind with mind, so terrorist organizations tend to eagerly grasp new trends and technology to update their methodology of attacks. COE-DAT drew attention to this topic in 2017 with the report of Dr. Afzal Ashraf & Dr. Anastasia Filippidou. According to the authors, terrorist organizations have effectively exploited technology, especially in social media. For example, Application Programming Interfaces (APIs) permit the majority processing of great volumes of the 'tweetstream' and because of this reason, they offer opportunities for event or sensuality detection surrounding a specific issue.[45]

Exploitation of big data requires swift and accurate sharing of information with proper members and organizations to make effective use. For example, the CIA found that the commercial sector's speed of data management innovation has surpassed that of US national agencies.[46]

Unmanned air vehicles (UAV) is another recently emerging technological challenge. Easy accessibility, manufacturability with 3D printer usage and low cost are the main advantages of UAVs, making their use attractive for terrorist organisations. Modern UAVs of today are relatively new and consist mainly of reconnaissance drones that were first conceived during the cold war period. There are many different categories, ranging from mini to decoy, with mass, range, flight altitude and endurance changing according to the model. The aircraft (or "drone", in common parlance) itself and its ground control unit are the main parts of UAV systems, and convey upon this technology the ability for the operator to remain separated from much of the risk experienced by the aircraft. While DAESH used drones for the first time in Syria in August 2014 for propaganda and reconnaissance purposes, the PKK/KCK terrorist organization used them for their swarm attack in November 2018. Different methods are used for defense against UAVs, such as radar, laser, and electromagnetic jamming. However, because of the difficulties in detecting UAVs with conventional aircraft-spotting methods, security forces need

[45] Ashraf, Afzal & Filippidou, Anastasia (2017). Terrorism and Technology. Centre of Excellence Defence Against Terrorism, https://www.tmmm.tsk.tr/publication/researches/05-TerrorismandTechnology.pdf (Accessed April 21, 2022).

[46] Simon Wibberly, Carl Miller (2014). "Detecting Events from Twitter: Situation Awareness in the Age of Social Media' in Christopher Hobbs, Matthew Moran and Daniel Salisbury (eds), Open Source Intelligence in the 21st Century, Basingstoke: Palgrave Macmillan, pp. 147-167

joint systems that have the capabilities to detect, localize and neutralize every kind of UAV. Human resources are a significant element in 24/7 surveillance, but multidisciplinary studies are also needed to provide a holistic approach.[47]

2.7. Cyber Domain and Security

In the last decade, private-sector and state entities have generally transitioned their administrative systems into the cyber domain to take advantage of developments that have occurred in the area of digitalization. Cyberspace's *sui generis* characteristics (temporality, physicality, permeation, fluidity, participation and attribution) have caused previously unexperienced feelings that people don't have in the so-called "real world". Traditional threats mitigated by traditional security methods have now been replaced by the new and newly merging threats of the cyber domain. One message in online social media can cause turmoil at the speed of light, and its impacts are greater than security agencies might traditionally expect. Terrorists, who are aware of the dangerous potentiality of the cyber domain, use this area to *enable*, *disrupt* and *destruct*. In order to provide sustainability and prevent vulnerability, the cyber domain must be handled with a holistic approach aimed at whole-system protection and enhanced resilience.[48]

In its "Good Practices Vol.1" Book, COE-DAT offers a new model: the Cyber Maturity Model. The Cyber Maturity Model is made up of ten domains: *Risk management and Resilience planning; Asset, Change and Configuration Management; Identity and Access Management; Threat and Vulnerability Management; Situational Awareness; Information Sharing and Communications; Event and Incident Response; Continuity of Operations; Supply Chain and External Dependencies Management; Workforce Management;* and *Cyber Security Program Management*.[49]

Risk management and resilience planning initially establishes a risk-management program to analyse and mitigate risks. To provide *asset management*, automated asset-management discovery tools are put into use. *Identity and access management* is the gate keeper and guard of the whole system. *Threat and vulnerability systems* evaluate the negligible, minor, moderate, major and catastrophic risks; prepare the system for attacks and warn the system itself and its

---

47 ŞEN, Osman & AKARSLAN, Hüseyin (2020). *"Terrorist Use of Unmanned Aerial Vehicles: Turkey's Example*". Defence Against Terrorism Review, Vol. 13, pp. 49- 85.

48 Yalcinkaya, Haldun (ed.) (2021), Good Practices in Counterterrorism, Ankara: Centre of Excellence Defence Against Terrorism.

49 Ibid, p. 71.

protection managers.[50] *Situational awareness* is the key factor to understand "the knowledge of where you are, where other friendly elements are, and the status, state, and location of the enemy".[51]

Information sharing and communication refine the communication skills of the involved parties, which might be relevant in the case of an emergency. *Event and incident response* is the component most highly related with situational awareness, and continuously observes the system for inner and outer dangers. *Supply chain and external dependencies management* mitigates the effects of interdependency. *Workforce management* is the construction of robust security culture among the personnel. *Cyber security program management* includes appropriate policies and paves the way to plan, implement, monitor, control, identify, and asses the risks in a continuous re-cycle model.[52]

In a nutshell, the Cyber Maturity Model's implementation in the cyber domain of critical infrastructures should keep those systems reasonably safe from the risks and attacks of terrorists. But it must not be forgotten that the key factor is the people who use this domain. The construct of a robust cyber security environment should be tackled in advance.

2.8. Media and Counter Terrorism

When examining the relationship between media and terrorism, it is critically important for NATO and partner nations to understand contemporary media, the information environment and how they intersect with security and terrorism. Terrorism and media have a symbiotic relationship. Traditional media, which can be defined as any form of mass communication used before the advent of digital media including TV, radio, newspapers and journals, can also convert into digital media via recent developments in technology.

Terrorists use media to *convey the propaganda of the deed, mobilize wider support for their cause,* recruit new followers, raise funds, plan future acts, communicate, conduct operations, gain publicity, and disrupt government response.[53] It has been said that terrorism is a combination of violence and communication.[54]

---

50 Ibid, p. 72-76.

51 Bennett, Brian T., (2007), *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, (Indiana: Wiley).

52 Ibid, p. 78-80.

53 Wilkinson, Paul, (1997), "The media and terrorism: A reassessment," *Terrorism and Political Violence*, Vol. 9, No. 2, pp. 51-64.

54 Yalcinkaya, Haldun (ed.) (2021), Good Practices in Counterterrorism, Ankara: Centre of Excellence

Terrorism needs a target audience, and the goal is to disseminate the message to more people than just those who were prone to terrorist attack. The media achieve an important role in propagating the news of attacks or even by directly conveying the message of terrorists. Terrorists also require media coverage in order to disseminate their message, compose fear and recruit new members. Therefore, the author suggests that the usage of media as a weapon by terrorist groups should be examined and observed thoroughly.

Since the late 1980s, the internet has proven to be a highly dynamic vehicle for communication, reaching now more than half of the global population as shown in Figure 4. Internet usage also increased the range of radicalization at the same time. Internet creates more opportunities to become radicalized, allows radicalization without physical contact, augments chances for self-radicalization, acts as a melting pot of different ideas and socialization place for the people, and accelerates radicalization process.[55]

In addition to platforms like Twitter, YouTube, and Google Earth, Metaverse is coming and will create new susceptibilities and deliver more opportunities to exploit them. Although not exhaustive, there are five ways the Metaverse will complicate efforts to counter terrorism and violent extremism. First is recruitment. Metaverse will likely create enormous opportunities for terrorist organizations, act as a capacity builder, and ease the ability to find people with like ideological opinions regarding the unlawful use of force against innocent people. Second is coordination; Metaverse offers new ways to coordinate, plan and execute acts of destruction across a diffuse membership. The third is new targets, which will bring new virtual and mixed reality spaces. Although some people claim that without physical reality there is no need to fear, as Nike prepares to sell **virtual shoes, it is critical to recognize the** very real money **that will be spent in the** Metaverse. With actual money comes real jobs, and with real jobs comes the potential for losing very real livelihoods. The fourth is propaganda. Like the current social media platforms, Metaverse can be used as a tool for disinformation. The last is armed training. Like a computer game, Metaverse will also provide a convenient habitat for all manner of operational drills without time-consuming travel and with low cost.

Defence Against Terrorism.

55 Nasraoui, A. (2021). Cyber Radicalization in the Digital Era in the MENA Region: The Case of.

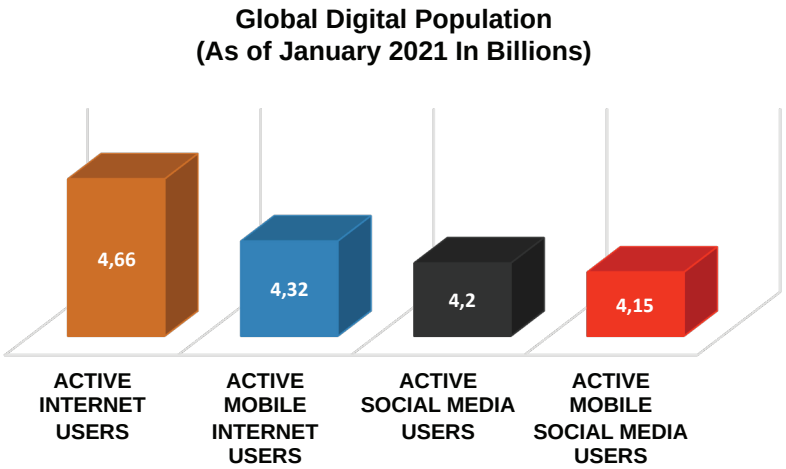


Figure 4. Global Digital Population (www.statista.com, Accessed April 22, 2022).

In order to prevent the usage of media platforms by terrorist organizations as a recruitment and communication area, states began collaborating with each other on building establishments to observe and share data. After 2020, the new age of web 4.0 began; this age needs advanced software development techniques based on AI. Open Source Intelligence (OSINT) is a useful way to detect and deter terrorists, but it requires the capability to manage large sets of data. A recent analytical brief by the United Nations CT Committee Executive Directorate (CTED) articulated many challenges on deciding whether and how to engage in countering terrorist narratives online, including criticism of the lack of monitoring and evaluation of counter-narrative initiatives.[56]

Learning lessons from successful public health initiatives, public-private partnerships – especially those related to critical infrastructure and security – and individualized campaigns can be a best practice in CT. Also, it is recommended that the principle of *"Politics has Primacy"* should be applied to CT media strategies so that they are subordinate to and aligned with the CT political narrative.[57]

---

[56] UNSC Counter-Terrorism Committee Executive Directorate, *CTED Analytical Brief.*

[57] Ashraf, Afzal & Foggett, Stephanie (2021). Media and Counter-Terrorism. Yalcinkaya, Haldun (ed.) (2021), Good Practices in Counterterrorism, Ankara: Centre of Excellence Defence Against Terrorism.

2.9. Pandemics and Bio-Terrorism

Bioterrorism is described as the deliberate release of biological agents to produce illness or death in people, animals, and plants.[58] The COVID-19 pandemic has cast a spotlight on bioterrorism, which has been accepted by most scholars as potential global threat.[59]

NATO nations have played a critical role during the pandemic, supporting Alliance, partner and other countries with expertise and advice as well as major medical, logistical and transport support. Military factories quickly adapted to the new situation and began to produce Personnel Protection Equipment (PPE), transform field hospitals into pandemic hospitals and use military logistic systems to support supply chains that were needed for the transportation of medicine and vaccines. NATO supported civilian authorities during the pandemic with Military Aid to Civilian Authority (MACA) operations, while protecting its personnel, continuing operations and maintaining collective security.[60]

The COVID-19 pandemic has revealed challenges that affect counterterrorism. It has become essential to understand terrorists' exploitation of the economic, social, and political impacts of various state responses to the disease. From the economic perspective, the pandemic has bestowed upon states the heaviest economic burden since the 1929 Great Depression.[61] Terrorist organizations tried to abuse this economically weak position to enhance social vulnerability. Although the effects of COVID-19 made life hard for all in its wake, most terrorist groups managed to keep the pace of their operational tempo, and in some cases even increased their impact by transforming risks into opportunities. Terrorist organizations exploited COVID-19 to emphasize the corruption in government responses and dis-inform people about the measures taken by states.

While most terrorist organizations exploited the COVID-19 pandemic in the ways detailed above, there were also outliers. These included the Afghan Taliban, who allowed health workers into their areas, and at the other extreme, Racially

---

58 O'Brien, C., Varty, K., & Ignaszak, A. (2021). The electrochemical detection of bioterrorism agents: a review of the detection, diagnostics, and implementation of sensors in biosafety programs for Class A bioweapons. *Microsystems & nanoengineering*, *7*(1), 1-19.

59 Dass, R. A. S. (2021). Bioterrorism. *Counter Terrorist Trends and Analyses*, *13*(2), 16-23.

60 Developments in terrorism & counterterrorism during the COVID-19 pandemic and implications for the future (2021). Research Report, COE-DAT, Ankara.

61 https://www.bbc.com/news/business-52236936 (Accessed 20, May 2022).

& Ethnically Motivated Violent Extremist (REMVE) groups who exploited both circumstances and technology on a scale not seen amongst other groups.[62]

Besides these effects, COVID-19 has created a significant challenge by opening a window to bioterrorism for terrorists. National interests must be informed by international interests; NATO and others must not permit terrorist organizations to find and use biological weapons against states. Bioterrorism, which has low cost, easy obtainability and transferability and potentially widespread and invisible impact, has attracted terrorist groups. In order to fight against this kind of terrorism, states need more collaboration than ever before. COVID-19 has once again articulated that NATO needs to adapt the lessons learned from the pandemic, and NATO *must* continue to maintain its primary objective of collective security against both state and sub-state actors. An environment that provides knowledge and best practice sharing is best suited for developing more innovative and coordinated strategic communication methods.[63]

COVID-19 has also increased the hate and violence feelings against immigrants. It is frankly apparent that terrorist organizations, especially right-wing extremist organizations, have become more vocal in anti-immigrant discourse and exploited social vulnerabilities created by the pandemic. Mutually coordinated immigrant policies are also needed to construct closer integration between military and civilian responders around “Total Defence” in a comprehensive, whole-of-society approach to further bioterrorism threats.[64]

3. Discussion and Conclusion

As one of the NATO accredited Centres of Excellence, COE-DAT continues to be effective in counter-terrorism concept and doctrine development, as capacity builder in the Education & Training pillar, and as Department Head (DH) of CT in global programming. COE-DAT is the cooperative venture of nine nations (Türkiye, Albania, Germany, Hungary, Italy, Netherlands, Romania, UK, and USA) . The Centre’s cumulative expertise and knowledge, collected since the day of its inauguration, continues to make progress every day with the dedicated contributions of the Centre’s staff.

---

62 Ibid, p. 67.
63 Ibid, p. 68.
64 Ibid, p. 69.

As stated before, COE-DAT has added great value to NATO's CT discipline by conducting courses, METs, seminars, workshops, conferences, and projects. It is impossible to detail all information that has been collected since 2004 in this small article. However, while scrutinizing all of the products in advance, the author found that some of the Centre's older key findings are now obsolete. Thus, COE-DAT's efforts in future programs of work will now focus on the the seven areas mentioned in the second part of this article.

In the "Global Counter-Terrorism Strategy" section, it is strongly recommended that countering violent extremism (CVE) and preventing violent extremism (PVE) be considered in parallel with CT efforts. Furthermore, radically and ethnically violent extremism (RMVEs), political terrorism, and domestic terrorism are new challenges in defense against terrorism. While GTI's top four terror groups are still religiously motivated, and the overwhelming number of deaths year on year are still from religiously motivated groups, countries should take heed of the newly emerging threats.

In the nuclear terrorism section, in order to prevent nuclear terrorism, the recommendation is to incorporate neural and social networks with system dynamics, using data mining systems through cloud computing technology, to enable systematic research on cell phones against possible terrorist incidents. That section also recommends using big data and AI to provide security and resilience.

When terrorism financing and cryptocurrencies are considered, the author encourages both national and international establishments to observe the flow of currency, to share knowledge, and to collaborate intelligently.

It is clear that women add value in all aspects of countering terrorism, including analysis, field work, and policy development. In addition, women are involved in the same extremist activities as men are, acting as sympathizers, supporters, radicalizers, recruiters, facilitators, perpetrators, enablers, and combatants. Women also act as agents to predict and prevent radicalization and terrorism and are critical security actors that act as force multipliers to build trust and increase security. Women's representation at all levels in the Security Sector should be increased. Counter-terrorism programming should be inclusive through a whole-of-government approach to consider gendered impacts and needs. DDR programs must include gender-sensitive policies and access to rehabilitation, training, and

job opportunities to break the cycle of violence, or they will not work for women. When re-integrating women, the key factor is the support of the community. Women must play a role in all stages of the DDR process. Women's agency in terrorism must be acknowledged, including analysis of the ways in which women provide material support to terrorist groups in a given place and context. Gender biases and stereotypes overshadow the power of women in terms of their engagement in terrorism, and these biases lead to the miscalculation of the threat posed by women. Capacity Building in CT is the main contribution of COE-DAT for NATO's Education & Training pillar. While COVID-19 interrupted some education efforts, COE-DAT swiftly adapted to the new situation and started providing virtual course models. The main challenge of virtual courses is that it is very hard to transform the learned content into practical application. Therefore, COE-DAT intends to start a project for "Terrorism Exercise Scenario and CT Simulation Development" next year. When courses return residential format in the near future, this project will give COE-DAT the opportunity to develop the skills of participants and help them apply their knowledge in practice. This project will also enhance the ability of COE-DAT to write more effective CT concepts and doctrine.

Social media, big data and UAVs are significant terrorist threats that are still in widespread use by terrorists. It is estimated that these challenges will continue in the near-term future. In addition to identifying and studying these trends, COE-DAT also has completed a horizontal scan for the far-term future, embarking on a new research project, "Emerging Threats in CT". In this project, the main aim is to use an interdisciplinary and holistic approach to bring scholars from different areas together in order to discuss future CT threats. Additionally, in the preparatory phases of this study, young people will be asked for their ideas about ontological security and fear of terrorism.

The Cyber domain seems to be one of the most dangerous facets of defence against terrorism. The new Cyber Maturity Model's implementation on the cyber domain of critical infrastructures is offered, and it is believed that this model may keep the system reasonably safe from the risks of being attacked by terrorists. However, the key factor is the people who use this domain. Constructing a robust cyber security environment presents a priority.

Media is a significant enabler for terrorist recruitment, propaganda and communication. OSINT and analysis of social networks can be effective in detecting terrorist activities. This will only be achieved by the international cooperation of related establishments. Besides current social media platforms, Metaverse will present opportunities for terrorists in the future, such as recruitment, coordination, new targets, propaganda and armed exercises. Learning lessons from successful public-private partnerships – especially those related to critical infrastructure and security – and individualized campaigns can be a best practice in CT.

The world was shocked by COVID-19 in 2019, and the impact of the pandemic, while it seems slowing down, is still ongoing. This calamity forced militaries and military industries to handle the situation and transform their capabilities into various areas, such as PPE production. On the other side, pandemics provide some opportunities for terrorists, and offer a "bioterrorism window". States need to intensify cooperation to follow the tracks of terrorist organizations in order to prevent unprecedented risks.

In addition to those mentioned in detail above, "Good Practices on Maritime Domain in CT", "Border Security in Contested Environment and Defence Against Terrorism", "Critical Infrastructure Security Resilience", "Struggle with Terrorism Financing" and "Special Operations Forces Roles in CT/Crisis Response" are all new project topics at COE-DAT, and work on these issues has recently begun in earnest.

COE-DAT, as in the past, will resolutely continue in its mission with great determination, always contributing more efforts in the CT domain. COE-DAT believes that one finger can easily be cut, but it is very hard to cut a fist. The joint intelligence of framework and sponsoring nations at the Centre will pave the way for a safer and more secure world.

Bibliography

Ashraf, Afzal & Filippidou, Anastasia (2017). Terrorism and Technology. Centre of Excellence Defence Against Terrorism, https://www.tmmm.tsk.tr/publication/researches/05-TerrorismandTechnology.pdf (Accessed April 21, 2022).

Ashraf, Afzal & Foggett, Stephanie (2021). Media and Counter-Terrorism. Yalcinkaya, Haldun (ed.) (2021), Good Practices in Counterterrorism, Ankara: Centre of Excellence Defence Against Terrorism.

Bennett, Brian T., (2007). *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, (Indiana: Wiley).

Brill, A. & Keene, L. (2014). *"Cryptocurrencies: The Next Generation of Terrorist Financing?"*, Defence Against Terrorism Review, Vol. 6, No. 1, pp. 7- 30.

"Brussels Summit Declaration" (2018), NATO, para 10, at https://www.nato.int/cps/en/natohq/ official _texts_ 156624.htm 9 (Accessed April 20, 2022).

Çambel, Hasan Cemil (1939). Belleten, Türk Tarih Kurumu Yayınları, Cilt:3, Sayı:10, 272.

Cameron, G. (1999). Nuclear terrorism: A threat assessment for the 21st century. Springer.

Dass, R. A. S. (2021). Bioterrorism. *Counter Terrorist Trends and Analyses*, *13*(2), 16-23.

Davidian, Alison (2019). Women in Terrorism and Counterterrorism, Workshop Report of COE-DAT.

Davis, J. (2011). The crypto-currency. *The New Yorker*, *87*.

Davis, J., West, L., & Amarasingam, A. (2021). Measuring Impact, Uncovering Bias? Citation Analysis of Literature on Women in Terrorism. *Perspectives on Terrorism*, *15*(2), 58-76.

Developments in terrorism & counterterrorism during the COVID-19 pandemic and implications for the future (2021). Research Report, COE-DAT, Ankara.

"Female Operators: Women in Special Forces"*, Jane's IHS Markit*, 2017, https://www.janes.com/images/assets/262/68262/Female_operators_Women_in_special_forces_edit.pdf (Accessed April 23, 2022).

Genna, Federica (2018). "*NATO's Enhanced Role in Counter Terrorism*", Defence Against Terrorism Review, Vol. 10, pp. 9- 21.

https://asean.org/wp-content/uploads/2021/01/ASEAN-Documents-on-Combating-Transnational-Crime-and-Terrorism-1.pdf (Accessed April 20, 2022).

https://www.bbc.com/news/business-52236936 (Accessed 20, May 2022).

https://cointelegraph.com/news/self-regulatory-organizations-growing-alongside-new-u-s-crypto-regulation (Accessed April 20, 2022).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0371&rid=6 (Accessed April 20, 2022).

https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF%2025%20years.pdf (Accessed April 19, 2022).

https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (Accessed April 20, 2022).

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/ct-policy-guidelines.pdf (Accessed April 20, 2022).

https://www.nato.int/nato_static_fl2014/assets/pdf/topics_pdf/20160905_160905-mc-concept-ct.pdf (Accessed April 20, 2022).

https://www.nato.int/nato-welcome/index.html (Accessed April 18, 2022).

https://www.nato.int/wearenato/why-was-nato-founded.html (Accessed May 15, 2022).

https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%202021%20there,the%20internet%20via%20mobile%20devices (Accessed April 22, 2022).

https://home.treasury.gov/system/files/136 nationalstrategyforcombatingterroristandother-illicitfinancing.pdf (Accessed April 20, 2022).

http://www.treasury.gov.za/publications/other/Mutual-Evaluation-Report-South-Africa.pdf (Accessed April 20, 2022).

https://www.unodc.org/documents/terrorism/Handbook_on_Criminal_Justice_Responses_to_Terrorism_en.pdf (Accessed April 20, 2022).

https://www.visionofhumanity.org/maps/global-terrorism-index/#/ (Accessed April 18, 2022).

https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web.pdf (Accessed April 20, 2022).

Jang, K. B., Baek, C. H., Kim, J. M., Baek, H. H., & Woo, T. H. (2021). Internet of Things (IoT) Based Modeling for Dynamic Security in Nuclear Systems with Data Mining Strategy. *Journal of The Korea Internet of Things Society*, *7*(1), 9-19.

Jens Stoltenberg, "The Secretary General's Annual Report 2017", NATO, at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_03/20180315_SG_AnnualReport_en.pdf (Accessed April 21, 2022).

Matthew Bunn. Preventing a Nuclear 9/11 Archived 2014-03-01 at the Wayback Machine Issues in Science and Technology, Winter 2005, p. v.

Medcalf J. (2005). NATO: Beginners Guides. Oneworld Publications, Oxford.

Mishra, R. (2021). Nuclear Terrorism: Statutory Shortcomings and Prosecutorial Opportunities. *International Law Studies*, *97*(1), 23.

Nasraoui, A. (2021). Cyber Radicalization in the Digital Era in the MENA Region: The Case of.

NATO, "BI-SC Collective Training and Exercise Directive (CT&ED) 075-003", 2 October 2013.

Nuclear Terrorism: Frequently Asked Questions, Belfer Center for Science and International Affairs https://www.belfercenter.org/publication/nuclear-terrorism-faq (Accessed May 16, 2022).

O'Brien, C., Varty, K., & Ignaszak, A. (2021). The electrochemical detection of bioterrorism agents: a review of the detection, diagnostics, and implementation of sensors in biosafety programs for Class A bioweapons. *Microsystems & nanoengineering*, *7*(1), 1-19.

Sadık, Giray & Bekçi, Eda (2019). *"NATO Capacity Building in Counterterrorism and Transatlantic Cooperation",* Defence Against Terrorism Review, Vol. 11, pp. 45- 63.

Schmid, A. P., Forest, J. J., & Lowe, T. (2021). Terrorism Studies. *Perspectives on Terrorism*, *15*(3), 142-152.

Simon Wibberly, Carl Miller (2014). "Detecting Events from Twitter: Situation Awareness in the Age of Social Media' in Christopher Hobbs, Matthew Moran and Daniel Salisbury (eds), Open Source Intelligence in the 21st Century, Basingstoke: Palgrave Macmillan, pp. 147-167

Şahin, G. (2017). Küresel Güvenliğin Dönüşümü; NATO Bağlamında Kavramsal, Tarihsel ve Teorik Bir Analiz. *Savunma Bilimleri Dergisi*, *16*(2), 59-81.

ŞEN, Osman & AKARSLAN, Hüseyin (2020). *"Terrorist Use of Unmanned Aerial Vehicles: Turkey's Example".* Defence Against Terrorism Review, Vol. 13, pp. 49- 85.

United Nations Office for Disaster Risk Reduction, "Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction", (2009), p.12

UNSC Counter-Terrorism Committee Executive Directorate, *CTED Analytical Brief.*

Voica, Dan-Radu & Kibaroğlu, M. (Ed.) (2010). Response to Nuclear and Radiological Terrorism, NATO Science for Peace and Security Series E.Human and Societal Dynamics, Vol.2, IOS Press BV, Netherlands.

Volders, B. (2021). *The Nuclear Terrorism Threat: An Organisational Approach*. Routledge.

Wharton, A. S. (2009). *The sociology of gender: An introduction to theory and research*. John Wiley & Sons.

Wilkinson, Paul, (1997), "The media and terrorism: A reassessment," *Terrorism and Political Violence*, Vol. 9, No. 2, pp. 51-64.

Women in Terrorism and Counterterrorism Workshop Report (2019). COE-DAT, https://www.tmmm.tsk.tr/publication/workshop_reports/08WomenInTerrorismAndCounterterrorism.pdf (Accessed April 20, 2022).

Yalcinkaya, Haldun (ed.) (2021), Good Practices in Counterterrorism, Ankara: Centre of Excellence Defence Against Terrorism.

Yıldız, Seda Öz (2019). Women in Terrorism and Counterterrorism, Workshop Report of COE-DAT.

Zizola, Anna (2019). Women in Terrorism and Counterterrorism, Workshop Report of COE-DAT.

E-DATR, 2022; 16 : 35-68
ISSN 1307 - 9190

Internet-Supported Recruitment of Terrorist Organizations: An Analysis of the Early Stages of the Recruitment Process and Countermeasures to Prevent Terrorist Recruitment[1]

Özgür Gürbüz[2]

Abstract: *Terrorism is one of the most critical threats to the stability of democratic societies. It seeks to achieve its political goals by undermining public trust in governments and instilling fear in society. Terrorist organizations need weapons and money for the continuity of their activities and to achieve their goals. However, terrorist organizations that do not have sufficient and qualified human resources are destined to disappear. For this reason, terrorist organizations adapted their recruitment processes to the rapid developments in internet-based technologies, and especially by using online social networks, gained significant momentum in their activities. They use internet-based technologies to help their traditional recruitment processes. By reorganizing their recruitment methods, all citizens of the world become their target audience. Moreover, they now carry out their recruitment processes more confidentially and faster than before, thanks to the communication opportunities provided by internet-based technologies. This study examines how terrorist organizations perform their internet-supported recruitment process, what tools they use, and*

[1] This study was carried out as part of the Research Assistantship Program held by COE-DAT between December 13th, 2021, and July 21st, 2022.

[2] Captain (TUR A), MA in Politics and Social Sciences, Research Assistant in NATO Centre of Excellence-Defence Against Terrorism, oz.gurbuz@hotmail.com

how the authorities can combat the recruitment of terrorist organizations by intervening in the early stages of the process. In the introduction part of the study, the relationship between terrorism, the media, and the internet are analyzed from a historical perspective to understand the recruitment process better. The second part examines the internet-supported recruitment process with its stages and the internet-based tools used in the process. It will also be mentioned that throughout the study, the internet-supported recruitment process is not defined as a different process from traditional recruitment but as complementary to each other. The last part analyzes how the human resources of terrorism can be rendered dysfunctional with countermeasures and practices developed at the initial stage of the internet-supported recruitment process, in which the bond between recruiters and potential candidates is not strengthened and is not confidential yet. As a result, this research essentially aims to reveal that the human resources of terrorist organizations can be weakened much more effectively with the national and international countermeasures and practices taken at the very beginning of the internet-supported recruitment process.

Key Words: *Terrorism, Internet-Supported Recruitment, Radicalization, Online Social Networks, Countermeasures.*

1. Introduction

Terrorism does not have a specific and widely accepted definition due to the nations' political interests and ideological pressure.[3] The well-known statement that "one's man terrorist is another man's freedom fighter" clearly implies the difficulty in defining terrorism objectively.[4] Although almost every country condemns terrorism, it is understood to be hard to define because it is an issue that can be distorted. Schmid and Jongman, in their research, showed that there were more than 109 definitions of terrorism in the literature.[5] According to Bruce Hoffman who is the editor- in-chief of Studies in Conflict and Terrorism:

---

3 Hayati Hazır, *Demokrasilerde İstikrarsızlığın Sebebi Olarak Siyasal Şiddet ve Terörizm,* (Nobel Yayın Dağıtım, 2001), p. 45.

4 Brian M. Jenkins, "International Terrorism The Other World War," (RAND Publication Series, A Project AIR FORCE Report Prepared for the United States Air Force, November 1985), p. 3.

5 Alex P. Schmid and Albert J. Jongman, et al., Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases and Literature, (Transaction Publishers, 1988), p. 6.

> "Terrorism is ineluctably political in aims and motives, violent – or, equally important, threatens violence, designed to have far-reaching psychological repercussions beyond the immediate victim or target, conducted by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia), and perpetrated by a subnational group or non-state entity." [6]

The impact and extent of terrorism cannot be measured solely by the number of victims it receives. In reality, terrorism has a greater goal than increasing the number of victims, such as destabilizing democratic societies and demonstrating the weakness of governments.[7] For this reason, *psychology* is the central strategy of terrorism, which means terrorist organizations are waging psychological warfare to gain their political goals. Thus, violence is used as a means of communication in this warfare.[8] Moreover, *publicity* is necessary for terrorism since terrorist organizations do not aim to directly or legally influence policy changes. Instead, they use violence to push societies toward responsible institutions indirectly.[9] For this reason, terrorist organizations struggle to control their target audience by using media as a weapon. German General Erich Ludendorff emphasizes the reality of media during World War I with his meaningful statement; "Wars are no longer being waged with weapons, but with words. The one who uses the word well, not the weapons, wins the war."

Terrorism tries to reach its ideological and political goals by creating fear, despair, and panic in society and coercing the authorities to take a step in their desired direction. Media is one of the most important tools to realize these purposes because terrorist acts that do not attract the media and the public's attention cannot reach their goal. Therefore, the issue of how to draw society's attention, as well as conventional and social media, has become much more essential for terrorist organizations than planning the action itself. In this regard, all the means of media are used by terrorist organizations to quickly deliver their terrorist acts and consequences to the masses and keep the public busy for days.[10]

---

6 Bruce Hoffman, Inside Terrorism, (New York: Columbia University Press, 2006), p. 43.

7 Walter Laqueur, "Reflections on Terrorism," Foreign Affairs, 65 (1) (1986), pp. 86-100, p. 87.

8 Ertan Efegil, *Terörizm ve Terörle Mücadele Yöntemleri*, (Gündoğan Yayınları, 2019), p. 25.

9 William F. Shughart II, "Analytical History of Terrorism, 1945-2000," Public Choice, 128 (1/2) (2006), pp. 7-39, p. 7.

10 Yusuf Devran, "The Problematics of Media and Terror," Gumushane University E-Journal of Faculty of Communication, 3 (2015), pp. 84-95, p.85.

1.1. Terrorism and Media

Once powerless actors realized the influence of media on public opinion, they employed the asymmetric effect of media for their terrorist acts in a short time.[11] Therefore terrorist organizations want to benefit from the media as soft power since they know it is impossible to win the fight by only applying hard power.[12] The primary aim of terrorist organizations is to provoke societies against the state, which ultimately wants to engage the state in an endless war.[13] This approach is defined as a strategy of attrition,[14] and it is evident in the words of Ayman al-Zawahiri, who was al-Qaeda's second-in-command until his death: "We are in a battle, and more than half of this battle is taking place in the battlefield of the media."

Indeed, it is unthinkable for terrorism to keep the national and international public busy without the media because the media is accepted as the leading actor in political communication.[15] For years, terrorist organizations have tried to take part in the media to direct or influence the media, convey their messages to their target audience, and make their propaganda. In this context, terrorist organizations have established their traditional media[16] and, eventually, their online social media. Furthermore, terrorist organizations have become *"the media"* with the developments of internet-based communication technology that does not require high costs, such as forums, websites, video/photo sharing sites, and especially online social networks.[17] Hence terrorist organizations reorganized their asymmetrical strategy on a brand new basis.[18] Moreover, technological developments fundamentally have affected the relationship between terrorism and media. In the history of terrorism, the attacks on World Trade Centre and the Pentagon by al-Qaeda on September 11, 2001 (9/11) was a significant turning point. Since then, a new age of terrorism has emerged, bringing terrorism to the

---

11 Hasan D. Pekşen, "The Use of Media in the Transformation of Asymmetric Strategies: Common Logic, Different Methods," Güvenlik Bilimleri Dergisi, 10 (1) (2021), pp. 239-258, p. 240.

12 Zakir Avşar, "Media, Terror and Security in the Age of Internet," TRT Akademi, 2 (3) (2017), pp. 117-132, p. 118.

13 Pekşen, "The Use of Media in the Transformation of Asymmetric Strategies: Common Logic, Different Methods," p.244.

14 Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," International Security, 31 (1) (2006), pp. 49-80, p. 63.

15 Necdet Ekinci, "A Problem Growing in the Marsh Media: Terrorism," Karadeniz Sosyal Bilimler Dergisi, 8 (15) (2016), pp. 217-236, p. 219.

16 Devran, "The Problematics of Media and Terror," p. 90.

17 Avşar, "Media, Terror and Security in the Age of Internet," p.119-120.

18 Pekşen, "The Use of Media in the Transformation of Asymmetric Strategies: Common Logic, Different Methods," p.251.

top of the political agenda.[19] At that time, terrorism was not a recent phenomenon, but the point reached of terrorism terrified the whole world. Without considering the advance in internet technology, we cannot explain the extent of today's terrorism.

1.2. Terrorism and the Internet

Shima D. Keen describes the internet as a double-edged sword from the counter-terrorism perspective. To prevent terrorist organizations from achieving their strategic and operational goals, one side of the blade represents the cyber defense of national digital infrastructure, and the other represents the prevention of using the internet as a communication tool and propaganda tool.[20] By using the internet as a tool, terrorist organizations can easily escape the control mechanisms of traditional media and have the opportunity to disseminate their messages to their target audiences at an unprecedented speed. Moreover, this opportunity has increased the scope of the terrorist organizations' target audience at a rate they did not expect.[21] Contrary to the traditional media order, not only the state-based actors but everyone has become able to share their messages using the internet.[22] Therefore terrorist organizations no longer need traditional media institutions to disseminate their messages to their target audiences. Additionally, they have re-functionalized their media strategy and put it at the base of their political strategies. The relationship between media and asymmetric strategy has been moved to a further dimension with the help of new internet-based tools provided by internet technology. [23] Besides, online social networks made this fact possible more quickly and effectively.

The main reasons why terrorist organizations use the internet, especially online social networks, are

- easy accessibility,
- no censorship,
- little regulation,
- almost limitless target audience,

---

19 Shima D. Keene, "Terrorism and the Internet: a Double-edge Sword," Journal of Money Laundering Control, 14 (4) (2011), pp. 359-370, p. 360.

20 Ibid, p. 360.

21 Avşar, "Media, Terror and Security in the Age of Internet," p. 127.

22 Ibid, p. 126.

23 Pekşen, "The Use of Media in the Transformation of Asymmetric Strategies: Common Logic, Different Methods," p.253.

- the anonymity of communication,
- fast flow of information,
- inexpensive development and maintenance of a website/accounts of online social networks,
- a multimedia environment, and
- the ability to shape coverage in the traditional media.[24]

These valuable elements allow terrorist organizations to carry out their activities with minimal risk.

1.2.1. The use of the Internet for Terrorist Purposes

Terrorist organizations can use internet technologies, especially online social networks, for various purposes. Information is the basis of these usage purposes. Because of the internet and its facilities, terrorist organizations can obtain, control and assimilate the information in line with their goals, and disseminate it to their target audiences, even the entire world. [25] In this respect, terrorist organizations can achieve their goals by promoting their ideology through online social networks, which have an unlimited and cheap source of information. With the advent of decentralized and inexpensive global communication networks, terrorist organizations have had the opportunity to convey their messages to more audiences than they previously could not reach. [26] For this reason, online social networks have become their leading information provider.

Various classifications can be made regarding the usage of internet technologies by terrorist organizations. Nevertheless, it is crucial to make the following distinction. Firstly internet can be used as a weapon to the national and international digital infrastructure. Secondly, it can simplify terrorist acts, providing privacy and significant superiority to terrorist organizations. The first is a cyber defense concern, while the second is an issue that considerably adds to the presence and continuation of terrorist organizations. That is, the internet is used as both a weapon and a tool.

[24] Zsolt Haig and László Kovács, "New Way of Terrorism: Internet and Cyber-terrorism," Aarms Security 6 (4) (2007), pp. 659-671, p.660 and Gabriel Weimann, "How Modern Terrorism Uses the Internet," (United States Institute of Peace, Special Report, 2004), p. 3.

[25] Mihaela Marcu and Cristina Bălteanu, "Social Media-A Real Source of Proliferation of International Terrorism," Annales Universitatis Apulensis Series Oeconomica, 16 (1) (2014), pp. 162-169, p.162.

[26] James A. Lewis, "The Internet and Terrorism," Proceedings of American Society of International Law, 99 (2005), pp. 112-115, p. 113.

The terrorist use of the internet as a tool can be divided into various areas such as target selection, recruitment, radicalization, training, planning and coordination, publicity and propaganda, psychological warfare, fundraising, etc.[27]

1.2.2. WEB 2.0: Development of Internet Technology and Terrorist Presence

Internet is a phenomenon of the modern world and an integral part of our lives, affecting every aspect of human life. Abbreviated from *interconnected networks*, it is a global network system that enables people to reach each other continuously and interactively.[28] The invention of the internet was a turning point in human history as it changed our lives significantly. Although it first appeared as a computer network in 1969 due to ARPA (Advance Research Projects Agency)'s research, Dr. Tim Bernes-Lee put the world wide web, Web 1.0, into practice in 1991. In the beginning, the world wide web allowed users only to search and read information,[29] and there was no user interaction or content generation. In the late 1990s, shortly after Web 1.0 came into existence, terrorist organizations began using the new technology for their political and operational purposes.[30] In this regard, after Movimiento Revolucionario Tüpac Amaru (MRTA or Tüpac Amaru) had seized the Japanese embassy in Lima, Peru, on December 17th,1996, a new era in terrorism and media relations began. The terrorist organization's website, which had over 100 pages, informed the entire world and even mainstream media about the terrorist incident. It was the first time a terrorist organization broadcasted its messages to the world without the assistance of the mainstream media.[31] After Web 1.0 was put into practice, not specific terrorist organizations but all terrorist organizations were engaged in cyberspace and quickly discovered the value and importance of the internet.[32] At the beginning of the terrorist presence in cyberspace in 1998, 12 out of the 30 terrorist organizations accepted as foreign terrorist organizations had

27 United Nations, "The Use of The Internet for Terrorist Purposes," (United Nations Office on Drugs and Crime, 2012), p. 3-12 and Weimann, "How Modern Terrorism Uses the Internet," p. 2 and Keene, "Terrorism and the Internet: A Double-edge Sword," p.364.

28 Kaan Altınkaynak, "Sosyal Medyanın Kavramsal Çerçevesi ve Teknik Altyapısı," in Sosyal Medya Platformları (Mustafa Karaca ed., Anadolu University Press, 2019), pp. 3-15, p. 5.

29 Ibid, p.4.

30 Mark Taylor, "An Analysis of Online Terrorist Recruiting and Propaganda Strategies," E-International Relations, available at https://www.e-ir.info/2017/07/19/an-analysis-of-online-terrorist-recruiting-and-propaganda-strategies/ (accessed January 9th, 2022), p.1.

31 Dorothy E. Denning, *Terror's Web: How the Internet Is Transforming Terrorism*, in Handbook on Internet Crime (Yuonne Jewkes and Majid Yar eds., Willian Publishing, 2009), p. 2.

32 Lewis, "The Internet and Terrorism," p. 112.

their websites. By 2002, 18 terrorist organizations on the U.S. State Department's list of terrorist organizations had 29 active websites.[33] Consequently, the internet has become the fundamental tool for disseminating terrorist propaganda, recruiting new members, training, and fundraising.[34]

Web 2.0 is based on interactive user-generated content and was put into practice in 2004. Since then, the term "social media or online social networks" has been used as a synonym for Web 2.0.[35] Online social networks are the most significant applications of Web 2.0 and have profoundly affected human history. Thanks to this new technology, people can communicate interactively and anonymously and create online communities via websites like Wikipedia, Facebook, Youtube, Twitter, etc. Moreover, audiovisual productions have been decentralized thanks to these new internet-based tools.[36] However, it soon became apparent that this new technology could be utilized for political purposes, and it was not long before terrorist organizations discovered new opportunities from online social networks. Terrorist propaganda, primarily through online social networks, started to be seen in the 2000s when this new technology began to be used. Unlike Web 1.0 technology, online social networks have completely changed the relationship between terrorist recruiters and their target audience, increasing their ability to disseminate terrorist propaganda beyond the borders and making mass recruitment easier.[37]

Important research shows that by 2005 all 40 organizations that were agreed as terrorist organizations had their presence in cyberspace with more than 4500 websites.[38] Another study about the significance and implications of online social networks in spreading terrorism finds that 9 out of 10 terrorist operations on the internet are based on online social networks.[39] According to the reports of the University of Arizona's Dark Web project, almost all terrorist organizations, including those whose names have not even been heard by the world public, exist on the internet.[40] Today in the era of Web 3.0, almost all terrorist organizations continue their presence through one form of internet technology. Thousands of websites,

[33] Weimann, "How Modern Terrorism Uses the Internet," p. 2 and Denning, *Terror's Web: How the Internet Is Transforming Terrorism*, p. 3.

[34] Taylor, "An Analysis of Online Terrorist Recruiting and Propaganda Strategies," p.1.

[35] Altınkaynak, "Sosyal Medyanın Kavramsal Çerçevesi ve Teknik Altyapısı", p. 7.

[36] Ekinci, "A Problem Growing in the Marsh Media: Terrorism," p. 218.

[37] Taylor, "An Analysis of Online Terrorist Recruiting and Propaganda Strategies," p.1.

[38] Ibid., p.1.

[39] Marcu et al., "Social Media-A Real Source of Proliferation of International Terrorism," p. 162.

[40] United Nations Counter-Terrorism Implementation Task Force, "Countering the Use of the Internet for Terrorist Purposes-Legal and Technical Aspects" (CTITF Publication Series, 2011), p. 27.

countless online social network accounts, online forums, and chat rooms are used by terrorists and their supporters.[41] Furthermore, thanks to the new internet technology, terrorist organizations use not only their native languages but also several different languages for their terrorist acts.[42]

2. Internet-Supported Recruitment

Terrorist organizations had used traditional recruitment methods before discovering that new internet technology was beneficial for their recruitment processes. Traditional recruitment was limited to some geographical regions and a particular target audience due to the inadequacy and difficulty of communication.[43] Furthermore, terrorist organizations relied on traditional media tools such as broadcast media (television, radio) and print media (newspapers, magazines, etc.) to carry out their psychological war and propaganda. They also utilized face-to-face meeting techniques to increase their human resources.[44] For example, before the 9/11 attacks, the official recruitment of al-Qaeda was provided by their terror camps operating in Afghanistan. With the global war on terrorism, like other terrorist organizations, al-Qaeda also transformed its traditional recruitment methods into a looser, distributed, and interactive structure. After that, new candidates began to be exposed to jihadist propaganda to be recruited via the internet, which is used to disseminate propaganda and communicate between local recruiters and new candidates.[45] Furthermore, with the help of the internet and online social networks, terrorist organizations now use individual cells to increase the variety of disseminated messages and communication skills.[46]

Recruiters of terrorist organizations currently work independently from the center of the organizations and have the opportunity to live anywhere in the world. Moreover, they take advantage of reaching their target audience living anywhere

41 Vase Rusumanov, "The Use of Internet by Terrorist Organizations," Information & Security: An International Journal, 34 (2) (2016), pp. 137-150, p. 137.

42 Weimann, "How Modern Terrorism Uses the Internet," p. 3.

43 Ergül Çeliksoy and Smith Ouma, "Terrorist Use of the Internet," Bilişim Hukuk Dergisi, 2 (2019), pp. 243-267, p. 253.

44 Sara Zeiger and Joseph Gyte, "Prevention of Radicalization on Social Media and the Internet," in Handbook of Terrorism Prevention and Preparedness (Alex P. Schmid ed., The Hauge, NL: ICCT Press, 2020), pp. 358-395, p.360.

45 Martin Rudner, "'Electronic Jihad': The Internet as Al-Qaeda's Catalyst for Global Terror," Studies in Conflict & Terrorism, 40 (1) (2017), pp. 10-23, p. 15.

46 Zeiger et al., "Prevention of Radicalization on Social Media and the Internet," p. 360.

in the world previously close to them.[47] Thus, terrorist organizations have gained a decentralized structure. On the other hand, individuals who sympathize with the ideology of the terrorist organization and who cannot communicate directly with members of organizations because of geographically far from the headquarter now become potential members of the terrorist organization.[48] The developments in internet technology have made it possible for both recruiters and sympathizers to use opportunities provided by the internet.

Martin Rudner defines the internet as a catalyst that facilitates terrorist activities and describes the emerging threat environment by al-Qaeda as an "electronic jihad."[49] Another scholar Marc Sageman describes this threat environment as "Leaderless Jihad," which provides easy training and propaganda to terrorist organizations from a distance and even their homes. The internet equips the sympathizers and potential members of terrorist organizations with inspirational guidance.[50] Considering the point reached by terrorism stemming from technological innovations, many different analogies can be made to describe it. However, online recruitment efforts of terrorist organizations have two essential features. First, it is a gradual transition and a process that needs many stages. Secondly, the recruitment process depends on the effective use of online platforms such as websites, online social networks, forums, chat rooms, games, applications, etc., unlike traditional recruitment.[51] In this sense, instead of the traditional institutions such as training camps and minor group affiliates used for radicalization and training, it has begun to give way to online institutions due to the capability of the high level of anonymity and easy communication.[52]

Whether traditional or internet-supported, the recruitment process is dynamic and often includes radicalization. While radicalization is not intense in the early stages of the recruitment process, it becomes more intense after friendship and

---

47 Denning, "Terror's Web How Internet is Transforming Terrorism," p. 12.

48 Stuart Macdonald and David Mair, "Terrorism Online: A New Strategic Environment," in Terrorism Online: Politics, Law and Technology (Thomas Chen, Lee Jarvis and Stuart Macdonald eds., Routledge, 2015), p. 6.

49 Rudner, "'Electronic Jihad': The Internet as Al Qaeda's Catalyst for Global Terror," p. 14.

50 Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (University of Pennsylvania Press, 2008).

51 Gabriel Weimann, "The Emerging Role of Social Media in the Recruitment of Foreign Fighters," in Foreign Fighters under International Law and Beyond (Andrea de Guttry, Francesca Capone and Christophe Paulussen eds., T.M.C. Asser Press, 2016), pp. 77-95, p. 81.

52 Abdel R. Alzoubaidi, Doina Prodan-Palade, and Siddik Ekici, "Terrorist Recruitment and Counter Measures in the Cyber World," in Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operation, (Sıddık Ekici, Hüseyin Akdoğan, Eman Ragab, Ahmet Ekici and Richard Warnes, eds, IOS Press, 2016), pp. 55-66, p. 58.

trust are built between the recruiter and the potential candidate. Radicalization is a part of recruitment, but in fact, these two processes need to be differentiated.[53] Although there is no agreed definition of radicalization, it refers to a process of belief modification [54] in which several factors work to produce extremist outcomes.[55] On the other hand, recruitment is a dynamic process that takes place according to the evaluation criteria of both the prospective candidate and the recruiter. In this dynamic process, prospective candidate is encouraged or deterred from joining the terrorist organization.[56] According to Edgar Jones, recruitment "is often divided into push-factors (social, economic, and political factors that create a sense of injustice and discrimination) and pull-factors (sense of belonging to a cause or network, adventure, and an opportunity to do something worthwhile or heroic). [57]"

Furthermore, there are two types of online recruitment processes in internet-based terrorist recruitment: internet-supported recruitment and virtual self-recruitment.[58] At the center of this study, the former will be examined, and the latter, often referred to as lone wolves, will be excluded from this study and can be the subject of another study.

2.1. Internet-Supported Recruitment Process

Many studies explain the recruitment process of terrorist organizations, and almost all of these studies describe it as a multi-stage process that includes radicalization. Regardless of the recruitment process, this study aims to reveal effective methods to protect the target audience from radicalization rather than to describe this process entirely. Because once the target audience is identified, the countermeasures taken on time by authorities can prevent the radicalization of vulnerable individuals more effectively. Terrorist organizations need much more human resources to reach their political goals than their weapons and financial

---

53 Edgar Jones, "The Reception of Broadcast Terrorism: Recruitment and Radicalisation," International Review of Psychiatry, 29 (4) (2017), pp. 320-326, p. 322.

54 Peter R. Neumann, "The Trouble with Radicalization," International Affairs 89 (4) (2013), pp. 873-893.

55 Ahmet Sinan Yayla, "Prevention of Recruitment to Terrorism," in Handbook of Terrorism Prevention and Preparedness (Alex P. Schmid ed., The Hauge, NL: ICCT Press, 2020), pp. 412-463, p. 415.

56 Jones, "The Reception of Broadcast Terrorism: Recruitment and Radicalisation," p. 322.

57 Ibid, p. 323.

58 Peter R. Neumann and Brooke Rogers, "Recruitment and Mobilisation for Islamist Militant Movement in Europe," (The International Centre for the Study of Radicalisation and Political Violence (ICSR) at King's College London for the European Commission (Directorate General Justice, Freedom and Security)), pp. 49-53.

resources because human resources are critical for carrying out attacks and sustaining operations. Therefore it is essential to develop efficient counter-terrorism policies to prevent terrorist organizations from recruiting new members.[59] Counter-terrorism policies that intervene in the early stages of the recruitment process can make the survival of terrorist organizations much less possible. For this reason, it is necessary to mention the recruitment process of terrorist organizations briefly.

It is difficult to propose a one-size-fits-all recruitment approach employed by terrorist organizations because each terrorist organization follows a distinct recruitment process. Moreover, each terrorist organization uses different recruitment procedures for different target audiences. According to Gabriel Weimann recruitment process of terrorist organizations can roughly be divided into four stages: instruction, preparation, training, and launching.[60] In another study supported by RAND, Al-Qaida's recruitment model is defined as four stages: the net, the funnel, the infection, and the seed crystal.[61] Although the stages of the recruitment process are named differently in the literature, at the beginning of the process, there is a stage of identifying prospective candidates to make the first contact with them. And after this stage radicalization process starts. For this reason, it is crucial to describe the recruitment process for defense against terrorism. In this study, the very beginning of the recruitment process is examined, regardless of the whole recruitment process of terrorist organizations, because this study aims to render this process dysfunctional from the very beginning.

Terrorist organizations cannot mainly use internet-supported recruitment but also use traditional recruitment for their survival and human resources. With the opportunities provided by internet technology, internet tools contribute to the traditional recruitment process as a communication and propaganda tool. To put it simply, there are no two types of recruitment process used by terrorist organizations, and in fact, they use internet-supported recruitment as a complement to traditional one. The internet-supported recruitment process represents the starting point of the overall recruitment process and consists of two stages. After that, the process generally continues with the traditional recruitment methods. In this part of the study, firstly target audience of the internet-supported recruitment is examined, then its stages and the internet-based tools used in the process are analyzed in detail.

---

59 Scott Gerwehr and Sara Daly, "Al-Qaida: Terrorist selection and Recruitment," (RAND Publication Series, 2006), p. 73.

60 Weimann, "The Emerging Role of Social Media in the Recruitment of Foreign Fighters," p. 78.

61 Gerwehr et. al., "Al-Qaida: Terrorist selection and Recruitment," p. 83.

2.2. Target Audience of the Internet-Supported Recruitment

Terrorist organizations utilize the internet and online social networks as propaganda and communication tool. Almost all internet-based platforms and tools are used to identify prospective candidates and establish first contact with them. Thus, it is possible to develop trust-based relationships. Gabriel Weimann, who has been working on the use of the internet by terrorist organizations for more than ten years, defines the use of the internet for recruitment purposes as cyber-fatwas.[62] Before explaining the stages of the internet-supported recruitment process, the first question is who responds to cyber-fatwas mentioned by Gabriel Weimann, since determining the target audience of internet-supported recruitment is crucial.

Terrorist organizations can reach an unlimited target audience thanks to open-source websites and online social networks throughout the internet-supported recruitment process. For this reason, the recruiters of terrorist organizations aim to reach everyone, regardless of gender, age, faith, or geography, including thrill seekers, ideologically motivated individuals, lone wolves, and groups from not only the Middle East but also Western societies.[63] To illustrate, terrorist organizations such as al-Qaeda-affiliated al-Nusra Front and Daesh use the internet to recruit new members from Europe, North America, Australia, and elsewhere across the Muslim world.[64]

The active recruiters of terrorist organizations are between 40 and 50 years, and the involved terrorists are between 20 and 35 years. According to the studies on the captured terrorists, it is seen that the age range of terrorists is 18-32 years old and overwhelmingly male. Furthermore, most of those who joined terrorist organizations from developed countries are well-educated individuals from middle-class families.[65] On the other hand, more than half of internet and social online network users are between 22 and 44 years old.[66]

---

62 Gabriel Weimann, "Cyber-Fatwas and Terrorism," Studies in Conflict & Terrorism, 34 (10) (2011), pp. 765-781.

63 Weimann, "The Emerging Role of Social Media in the Recruitment of Foreign Fighters," p. 78.

64 "Foreign Jihadists in Syria: Tracking Recruitment Networks," The Washington Institute for Near East Policy, available at https://www.washingtoninstitute.org/policy-analysis/foreign-jihadists-syria-tracking-recruitmentnetworks (accessed April 23rd, 2022) and "Up to 11,000 Foreign Fighters in Syria; Steep Rise among Western Europeans," The Washington Institute for Near East Policy, available at https://www.washingtoninstitute. org/policy-analysis/11000-foreign-fighters-syria-steep-rise-among-western-europeans (accessed April 23rd, 2022).

65 Alzoubaidi et. al., "Terrorist Recruitment and Counter Measures in the Cyber World," p. 56.

66 Marcu et al., "Social Media-A Real Source of Proliferation of International Terrorism," p. 166.

Considering the relationship between the average age of those who joined terrorist organizations and internet users, it is seen that the main protagonists of internet-supported recruitment are the young generations. The internet is a tool used by terrorist recruiters to radicalize the youth rather than the older generation. It is easier to find individuals with a higher tendency to radicalize in the young generation because socially depressed, angry and marginalized individuals are more common among them. Also, the young generation is prone to spend more time online than others.[67] As a result, terrorist recruiters mainly aim to make the young generation the leading actor in the recruitment process because it is easy to reach them through the internet and online social networks.[68]

2.3. The Stages of Internet-Supported Recruitment

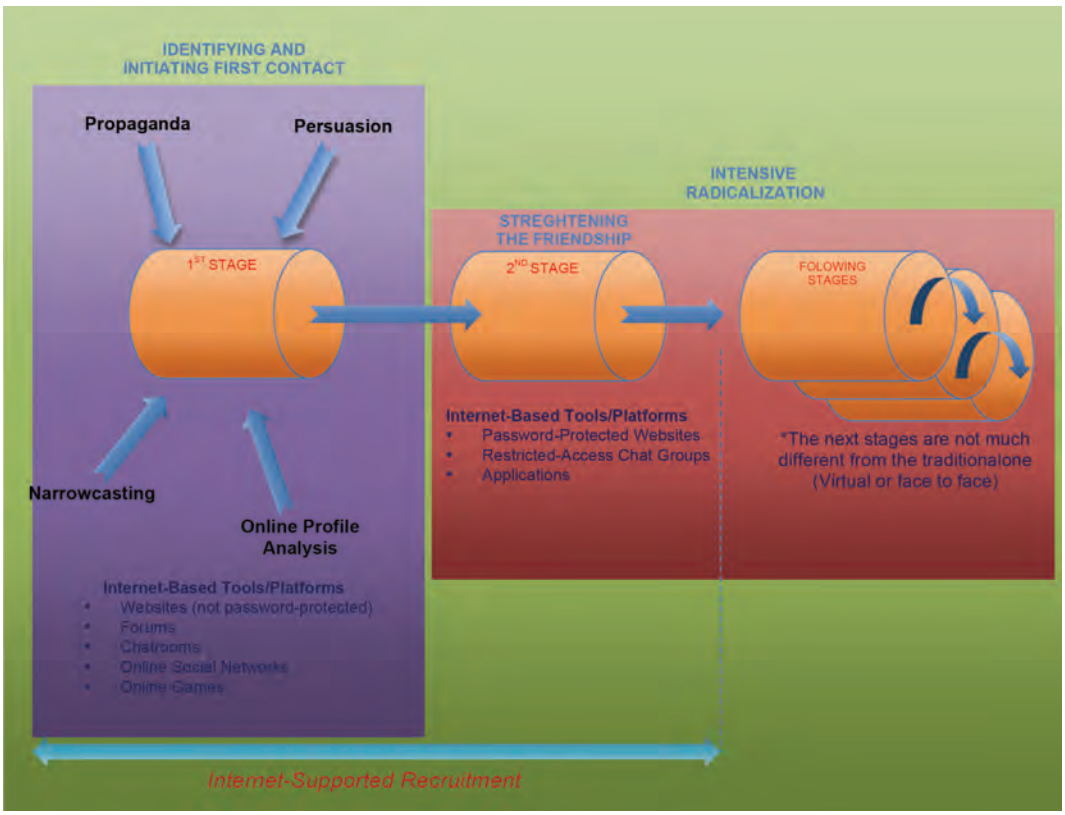


Figure 1. Internet-Supported Recruitment's Stages

[67] Tina Freiburger and Jeffrey S. Crane, "A Systematic Explanation of Terrorist Use of the Internet," International Journal of Cyber Criminology 2 (1) (2008), pp. 309-319, p. 313-314.

[68] Çeliksoy et. al., "Terrorist Use of the Internet," p. 254.

During the internet-supported recruitment process, terrorist organizations use all the opportunities provided by today's internet technology and can instantly adapt their recruitment processes to changing situations. In this regard, the internet and mainly online social networks are used for two purposes in the recruitment process. Moreover, these two objectives constitute two successive stages of the internet-supported recruitment process. The first one is using the internet and online social networks as a means of propaganda and increasing the visibility of the terrorist organization to identify prospective candidates. This stage can be described as *"Identifying and Initiating First Contact"* with the possible candidates.[69]

The second aim of using internet technologies by terrorist organizations is to radicalize the identified candidates who want to be a member of a terrorist organization. While these two purposes constitute the two stages of internet-supported recruitment, they also determine the entry points of prospective candidates into the recruitment process. The first stage can be skipped if the prospective candidate positively views joining a terrorist organization. After the first stage, monitoring the recruitment process can be difficult for the authorities because of the confidentiality provided by internet technology. Furthermore, it could be troublesome to disrupt and intervene in the process. As a result, this research aims to discourage potential candidates from proceeding to the second stage of the internet-supported recruitment process, referred to as *"Strengthening the Friendship."* Therefore, the countermeasures and practices taken towards the first stage of internet-supported recruitment can disrupt this process and minimize the efforts of terrorist organizations to recruit new members and provide significant advantages to the authorities in the defense against terrorism. In this regard, Figure-1 delivers a diagram of stages of internet-supported recruitment based on these purposes and shows the tools used in each stage.

There is no intensive radicalization throughout the first stage, *"Identifying and Initiating First Contact."* Internet-based tools such as online social networks, open-source websites, forums, and online games are utilized to disseminate propaganda, present personal narratives, and initiate first contact with potential and vulnerable candidates to prepare them for radicalization. It should be mentioned that these internet-based platforms are worthy of identifying and connecting with prospective candidates in addition to other benefits of internet-supported recruitment.[70] Methods

---

69 Yayla, "Prevention of Recruitment to Terrorism," p. 423.

70 Gregory Waters and Robert Postings, "Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook," (Counter Extremism Project (CEP) Report, 2018), p. 10-11.

such as persuasion, narrowcasting for a specific target audience, propaganda, and online profile analysis are used to identify and select vulnerable individuals.[71] However, using such platforms, especially online social networks for recruitment, provides advantages for the recruiters but also has disadvantages. Transparent and non-protected communication with a potential candidate on online social networks can leave recruiters and prospective candidates more open to police monitoring. Therefore efficient countermeasures and practices taken for turning individuals on this path can prevent terrorist organizations from recruiting new members since this stage is almost entirely done through open internet resources. Moreover, it is easier for the authorities to monitor and neutralize recruiters' efforts in the first stage.

In the second stage of internet-supported recruitment, once a recruiter identifies potential candidates, the recruitment process continues with more secure platforms such as password-protected websites and one-to-one messaging applications such as Whatsapp, Telegram, Kik, etc. Recruiters utilize unregulated mobile messaging apps and password-protected websites to accelerate radicalization while strengthening friendships and trust with possible candidates. After the first stage, it is much more difficult for authorities to infiltrate the recruitment process and reach victims because the second stage of internet-supported recruitment is done very confidentially.

Consequently, the intensity of radicalization and the degree of confidentiality of communication differentiate these two stages from each other. So it can be concluded that it is essential to develop efficient active and passive countermeasures in the first stage of internet-supported recruitment to prevent the recruitment of terrorist organizations. Also, this concludes that terrorist organizations use different types of internet-based tools in the different stages of the recruitment process. While some internet-based tools are used for spreading propaganda to a broader target audience, others help the recruiter guide individuals towards one-to-one, eventually, face-to-face communication.[72]

2.3.1. The First Stage: Identifying and Initiating First Contact

Terrorist organizations initially used internet-based technologies to disseminate propaganda, attract the international public's attention, and spread their organizational structure and ideologies. Moreover, they continue to use internet-based technologies for these purposes. While they achieve these goals by disseminating information

[71] Zeiger et. al., "Prevention of Radicalization on Social Media and the Internet," p.364

[72] Ibid, p. 365.

through websites and other tools,[73] usage purposes of the internet have increased with the opportunities provided by new internet-based platforms. Whether used as a propaganda tool or for further recruitment efforts, the internet and especially online social networks have facilitated terrorist organizations to spread their ideologies unprecedentedly and reach unlimited target audiences without geographical limitations.

Terrorist organizations increasingly use websites, chat rooms, and forums for propaganda and recruitment since such internet-based tools are successful in creating virtual communities.[74] Unradicalized passive candidates exposed to the materials on these platforms are simply readers rather than active members. For this reason, these kinds of venues powered by images and video clips are used to facilitate the radicalization of these individuals.[75] Recruiters can succeed in attracting the attention of those who sympathize with terrorist organizations via websites, chat rooms, and forums supported by digital materials. Many studies show that chat rooms and virtual meeting points bring individuals together and strengthen the recruiter's efforts in the recruitment and radicalization process.[76]

In their recruitment strategies, terrorist organizations have recently used online social networks such as Facebook, Twitter, Instagram, etc., because these platforms provide them with more opportunities than websites, chatrooms, and forums. As well as using mainstream online social networks, terrorist organizations use various online social networks such as Soundcloud, Vimeo, and Flickr.[77] For example, Al-Shabaab, whose recruiting efforts and trends are documented by studies,[78] successfully uses online social networks, chat rooms, and Youtube to contribute to its recruitment process. Platforms such as Facebook, Twitter, Instagram, etc., are used effectively in recruitment. But platforms with video content, such as Youtube, are used as the primary propaganda sources by terrorist organizations.[79] Recruiters mainly use these platforms to attract the attention of

---

73 Alzoubaidi et. al., "Terrorist Recruitment and Counter Measures in the Cyber World," p. 59-60.

74 Anna Stenersen, "The Internet: A Virtual Training Camp?," Terrorism and Political Violence, 20 (2) (2008), pp. 215-233.

75 Çeliksoy et al., "Terrorist Use of the Internet," p. 250.

76 Keene, "Terrorism and the Internet: a Double-edge Sword," p. 365.

77 Zeiger et al., "Prevention of Radicalization on Social Media and the Internet," p.364

78 Ken Menkhause, "Al-Shabaab and Social Media: A Double-Edged Sword," Brown Journal of World Affairs, 20 (2) (2014), pp. 309-327.

79 Eddy Lynton J., Gerg Gullion, and James L. Williams, "Countering Terrorist Recruitment: Social Media, Cyber Terror, and Peaceful Platforms," in Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operation, (Sıddık Ekici, Hüseyin Akdoğan, Eman Ragab, Ahmet Ekici and Richard Warnes, eds, IOS Press,2016), pp. 67-81, p. 70.

the young generation because the presence of young users provides an excellent ground to recruit and disseminate extremist ideologies.[80]

These platforms not only provide opportunities such as chatting, sharing clips, music, and documents but also provide terrorist recruiters to track those who log into these platforms. This way, the recruiter can narrow its target audience and reach a specific audience. By roaming online social networks or chatrooms, terrorist recruiters select prospective candidates by following those who access the content they upload and monitoring their activities.[81] With this simple method, recruiters can have personal data, interests, thoughts, and tendencies, which help them choose prospective candidates to recruit. Then recruiters send friend requests to suitable prospective candidates, and in this way, recruiters identify promising candidates for their organizations.[82] Efforts to gather information about prospective candidates lie at the heart of the internet-supported recruitment process. For this reason, all these kinds of online social networks and electronic bulletin boards can serve as a vehicle to reach prospective candidates, particularly the young generation.[83]

Furthermore, online games are designed and used by terrorist organizations to radicalize the young generation and to select future candidates. They use online games to attract their attention, so recruiters try to persuade prospective candidates by taking advantage of their weaknesses. Online games, which are offered in multiple languages, are used for recruitment and training. With these games, young prospective candidates are encouraged to use violence against states and prominent political figures to achieve virtual successes and then be motivated to adapt these successes to real life.[84] For example, "Special Force" and "Special Force 2," released by Hezbollah, are designed to spread the terrorist organization's values and ideas.[85] Another example is the "Quest for Bush game," released by The Global Islamic Media Front associated with al-Qaeda, which gives the young generation the goal of killing President George W. Bush. These are just a few examples of using online games as a platform for recruitment and radicalization of the game-loving young generation.[86]

---

80 Alzoubaidi et al., "Terrorist Recruitment and Counter Measures in the Cyber World," p. 60-61.

81 Weimann, "How Modern Terrorism Uses the Internet," p. 8.

82 Marcu et al., "Social Media-A Real Source of Proliferation of International Terrorism," p.162.

83 Weimann, "How Modern Terrorism Uses the Internet," p. 8.

84 United Nations, "The Use of The Internet for Terrorist Purposes," p. 5

85 Denning, *Terror's Web How Internet is Transforming Terrorism*, p. 15.

86 Rusumanov, "The Use of Internet by Terrorist Organizations," p. 144 and Zeiger et.al., "Prevention of Radicalization on Social Media and the Internet," p. 362.

Another advantage of internet-based technologies in the first stage of internet-supported recruitment is to help recruiters to overcome language challenges. Thanks to web providers, including Netscape and Internet Explorer, whichever language the internet user provider set, they can be directed to the content that the recruiters explicitly designed for internet users' native language. Hence this makes it easier for the recruiters to reach new prospective candidates from all nationalities and help to increase the target audience.[87]

2.3.2. The Second Stage: Strengthening the Friendship

When prospective candidates are convinced and gain the recruiter's trust, they are ready to move on to the second stage of the recruitment process. Password-protected internet tools and encrypted messaging services are used for intensive radicalization by recruiters in the second stage.[88] The difference between the second stage and the first stage is that prospective candidates now believe in the ideology of the terrorist organization. Therefore recruiters invite prospective candidates to the hidden pages of the internet and launch the intensive radicalization and training process.

In this stage, platforms such as password-protected websites and restricted-access internet chat groups are used as a means of clandestine recruitment.[89] Cyber platforms with restricted access and password protection offer a venue for recruiters to meet with prospective candidates for radicalization.[90] This privacy provided by internet-based technologies to terrorist organizations is called *Dark Web or Deep Net* in the literature.[91] The most important criterion for candidates to reach this recruitment stage and meet with members of a terrorist organization through such fully or partially restricted access platforms is either proof of their loyalty or recommendation from those members of the terrorist organization.[92]

Furthermore, we now witness that they can develop software for communication among themselves and even make some downloadable applications since the members of terrorist organizations need to communicate secretly. For example,

87 Keene, "Terrorism and the Internet: a Double-edge Sword," p. 365.

88 Zeiger et al., "Prevention of Radicalization on Social Media and the Internet," p. 366.

89 Gerwehr et al., "Al-Qaida: Terrorist selection and Recruitment," p. 83.

90 Denning, *Terror's Web How Internet is Transforming Terrorism*, p.15.

91 Lynton J. et al., "Countering Terrorist Recruitment: Social Media, Cyber Terror, and Peaceful Platforms," p. 70.

92 Marcu et al., "Social Media-A Real Source of Proliferation of International Terrorism," p.164.

Daesh released a free application called The Dawn of Glad Tidings, which could be downloaded from the android market. By using this application, members of Daesh and prospective candidates could receive instant information from the news about the organization. Once the application is downloaded, users can monitor and see tweets, links, hashtags, images, videos, and posts of specific accounts.[93] Besides, instead of special-downloadable applications, terrorist organizations also use well-known free messaging applications such as Telegram, which allows users to send text messages, voice messages, pictures, videos, and documents. Terrorist organizations prefer these applications because they provide their users secret messaging with an end-to-end encryption feature.[94]

2.4. Operating Principle of Internet-Supported Recruitment Process

One of the new emerging trends used by terrorist organizations in their recruitment process is narrowcasting.[95] In other words, terrorist organizations can shape their propaganda and persuasion processes according to their specific target audiences. In this process, they use different methods with the help of various internet-based tools instead of a one-size-fits-all approach. Moreover, they choose their internet-based tools according to the internet usage tendencies of their target audience. For example, the propaganda they make for those living in Europe is much different from the propaganda they make for those living in Muslim countries. Narratives they developed to recruit women are different from those designed for the young generation. Therefore, profile analysis is one of the most effective techniques that make possible narrowcasting for each target audience. For this reason, terrorist organizations try to reach personal data, tendencies, grievances, cultural symbols, and anthropological codes through the profile analysis that they make on the internet. And this is the beginning point of the first stage of the internet-supported recruitment process, actually the whole process. In this regard, Figure-2 provides a diagram about the process of internet-supported recruitment, which starts with profile analysis, continues with the narrowcasting for a specific target audience, and ends with building friendships by exploiting anthropological codes and manipulating grievances. So, The first stage of the internet-supported

---

93 "ISIL using Twitter App 'Dawn' to Keep Jihadists Updated," The Washington Times, available at https://www. washingtontimes.com/news/2014/jun/18/isil-using-twitter-app-dawn-keep-jihadists-updated/ (accessed April 24th, 2022).

94 Zeiger et al., "Prevention of Radicalization on Social Media and the Internet," p. 365.

95 Weimann, "The Emerging Role of Social Media in the Recruitment of Foreign Fighters," p.81.

recruitment process mainly consists of profile analysis, narrowcasting, and techniques used for building friendships.

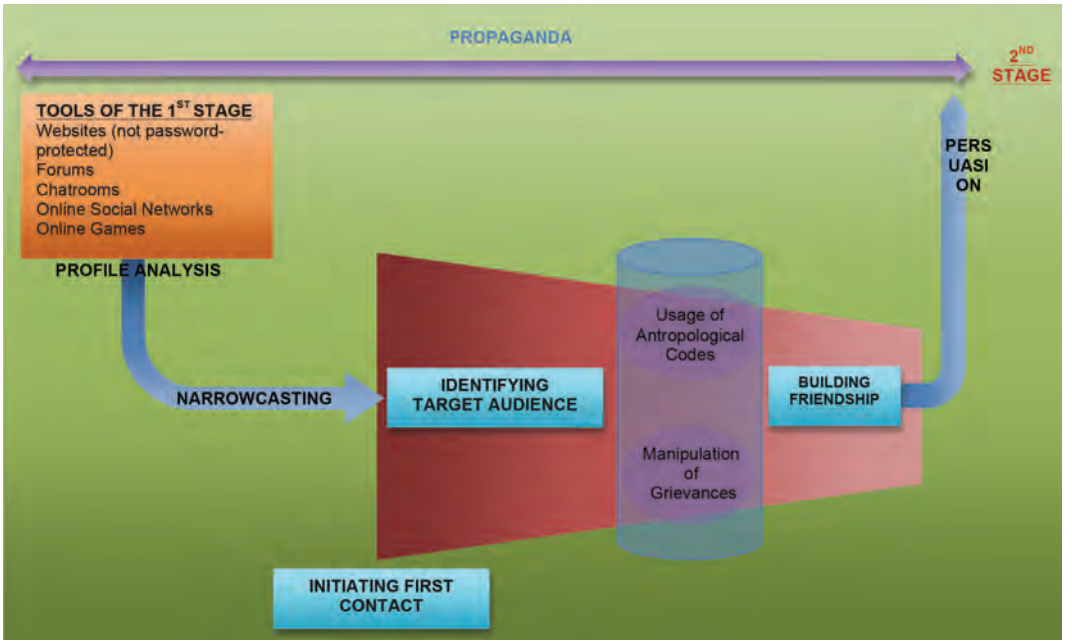


Figure 2. The First Stage of Internet-Supported Recruitment in Detail

2.4.1. Profile Analysis for Narrowcasting

All techniques used in the internet-supported recruitment process, from candidate selection to persuasion, aim to influence and guide vulnerable individuals' minds. As a communication tool, the internet is very effective for finding prospective candidates interested in the ideology of terrorist organizations and willing to support their terrorist activities. Moreover, due to group polarization, like-minded individuals can search for each other and reinforce their ideas and behaviors with the help of the fast communication capability of the internet.[96] The recruiter's essential purpose is to identify individuals who share their ideology and include them in the recruitment process. As a result, propaganda is valuable in identifying prospective candidates by utilizing all the opportunities provided by the internet.

When propaganda appeals to vulnerable individuals, the possibility of preventing them from becoming radicalized decreases gradually because terrorist narratives contain push and pull factors created by effective profile analysis methods.

[96] Alzoubaidi et al., "Terrorist Recruitment and Counter Measures in the Cyber World," p. 57.

This complex process is designed to capture the hearts and minds of vulnerable prospective candidates to mobilize and recruit them. For example, the media wing of the Daesh terrorist organization, Al-Hayat Media Center, portrays life within Daesh territory as a spiritually gratifying location while declaring European states of being immoral and unlawful to the possible target audience living in Europe. While terrorist organizations propagate through the dissatisfaction of their target audience, they try to include them in the recruitment process by offering them an alternative.[97]

Terrorist organizations use internet-based tools as a part of their propaganda throughout the first stage of the internet-supported recruitment process to convince prospective candidates. The first stage ultimately can be described as an election and selection part of the recruitment process in which individuals who are susceptible to the ideology of the terrorist organization are chosen. Therefore, profile analysis of the target audience is one of the most important instruments to identify candidates who respond to their propaganda and attract them to the persuasion process. With the help of profile analysis, terrorist organizations capture detailed information about those who browse and access websites, social media accounts, videos, movies, games, etc., created by recruiters. Then they use this information to develop their presentations and narratives.[98] Recruiters especially attach importance to profile analysis of online social media accounts such as Facebook, Twitter, and Instagram, which are used extensively by the young generation. For this reason, such platforms have become an open venue where terrorist recruiters look for prospective candidates for their human resources. By examining the personal profiles of such platforms, recruiters learn about personal interests and weaknesses.[99] In this way, recruiters convert their broader target audience into a specific target audience.

2.4.2. Narrowcasting and Recruitment

Recruiters, who identify their target audience with a detailed profile analysis, initiate first contact with them after determining the anthropological codes and grievances of the target audience. The ultimate goal of this narrowcasting, based on using anthropological codes of candidates and manipulating grievances, is to take the convinced individuals to the next stage. Effective persuasion techniques are used to achieve this goal, but the target audience must also be thoroughly

97 Logan Macnair and Richard Frank, "'To My Brothers in the West…': A Thematic Analysis of Videos Produced by the Islamic State's al-Hayat Media Center," Journal Contemporary Criminal Justice, 33 (3) (2017), pp. 234-253.

98 Weimann, "The Emerging Role of Social Media in the Recruitment of Foreign Fighters," p. 80.

99 Çiğdem Erdin, "Radikal Selefi Örgütlerin Sosyal Medya Kullanımı: IŞİD Örneği," Bilge Uluslararası Sosyal Araştırmalar Dergisi, 1 (2) (2017), pp. 124-130, p. 128.

researched. As a result, the narratives should contain strong messages. To achieve these objectives, recruiters embellish the process with symbols based on the anthropological codes of the candidates they select via the internet and exploit the target audience's grievances. In this respect, individuals and society's social anthropological codes originating from the past are crucial because these codes may have different meanings for each community. Likewise, beliefs, cultural values, and associations with high symbolic meaning can mobilize the masses. Each community can attach value to some symbols having historical and cultural importance, which are identified with that society.[100]

Social anthropological codes refer to physical and biological characteristics of the society, geographical weaknesses, belief systems, cultural sensitivities, symbols, attitudes and habits, memory breakdown, traumas, and so on.[101] However, demographic factors such as age and gender, as well as social and economic circumstances, can shape this stage.[102] The ultimate goal of this stage is to change the attitudes and behaviors of the target audience. The usage of propaganda by terrorist organizations is identical to the history of terrorism. Developments in internet-based technologies have changed the form and content of propaganda. Terrorist organizations now usually use websites, online social networks, chatrooms, online forums, movies, TV series, games, etc., to spread their ideologies and ideas to gather supporters and ultimately create the perception that they are "right." Furthermore, with the opportunities provided by internet technologies, they intensely use internet-based tools in the context of social anthropological codes.[103]

2.4.3. Exploiting Grievances

Terrorist organizations not only use the internet as a propaganda tool but also to manipulate people's grievances, especially the young generation who feel excluded from society. The target audience of terrorist organizations in their internet-supported recruitment strategies is generally vulnerable and marginalized groups. In this recruitment process, terrorist organizations typically prefer individuals who are humiliated and alienated in society.[104] Thanks to the communication opportunity

---

100 Sefer Darıcı and Ebru Karadoğan İsmayıl, "Popüler Kültür, Oyunlar ve Propaganda: Terörizmin Antropolojik Kodları", Bilge Strateji, 10 (19) (2018), pp. 39-65, p. 44-45.

101 Darıcı et al., "Popüler Kültür, Oyunlar ve Propaganda: Terörizmin Antropolojik Kodları," p. 45.

102 United Nations, "The Use of The Internet for Terrorist Purposes," p. 3.

103 Darıcı et. al., "Popüler Kültür, Oyunlar ve Propaganda: Terörizmin Antropolojik Kodları," p. 60.

104 European Commission's Expert Group on Violent Radicalisation, "Radicalisation Processes Leading to acts of Terrorism," (European Commission, 2008), p.13, available at https://www.clingendael.org/sites/ default/files/pdfs /20080500_cscp_report_vries.pdf (accessed May 3rd, 2022).

provided by the internet, it is not difficult for individuals to reach communities where they can make sense of their identities. Thus, the internet has become a valuable place that allows them to contact others for companionship and support.[105]

Terrorist organizations such as Daesh perform user profile analysis on online social networks such as Twitter and expertly use online hate as a propaganda and persuasion tool in their recruitment process.[106] For this reason, recruiters reaching the prospective candidate through online networks try to define prospective candidates as a loser and lonely individuals and hit their souls with promises by using their weaknesses and chosen traumas. Then the recruiter tries to convince them that only they can help them to establish a new order. After finding individuals who are psychologically depressed and looking for an environment to express themselves, terrorist organizations use these individuals for their terrorist purposes.[107]

Most of the time, the feelings of dissatisfied individuals are exploited throughout the recruitment process, and try to make them feel important and indispensable. In this process, the propaganda of the terrorist organization is supported by the facilities provided by the internet, especially videos, forums, Facebook, and Twitter posts. Furthermore, recruiters eventually try to persuade their target audience to pass to the second stage by establishing friendly relations. [108] During this procedure, there may be those eliminated and those who break away from the process. On the other hand, recruiters not only look for dissatisfied individuals when performing profile analysis but also try to reach adrenaline and excitement seekers and sympathizers, which are much easier to convince. [109]

Consequently, profile analysis is the most crucial milestone in the first stage of the internet-supported recruitment process because recruiters determine the target audience' anthropological codes and grievances in addition to just selecting the target audience as a result of profile analysis. The data obtained from this analysis constitutes all the propaganda developed during the first stage. Naturally, these processes are the foundation of the persuasion process.

---

105 Freiburger et. al., "A Systematic Explanation of Terrorist Use of the Internet," p. 310.

106 Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media," Social Science and Public Policy, 54 (2017), pp. 138-149, p.138.

107 Erdin, "Radikal Selefi Örgütlerin Sosyal Medya Kullanımı: IŞİD Örneği," p. 129

108 Awan, "Cyber-Extremism: Isis and the Power of Social Media," p. 139

109 Ibid, p. 148.

3. Countermeasures to Prevent Recruitment Efforts of Terrorist Organizations

Terrorist organizations, which continue their recruitment efforts with the support of the internet according to the developing and changing world conditions, now have an unlimited target audience for their human resources. The younger generations, who spend most of their time on the internet, are more vulnerable to terrorist organization propaganda and continue to be the leading actors in this process. For this reason, countermeasures and practices limiting terrorist organizations' access to human resources can provide numerous benefits to authorities because terrorist organizations require more human resources to use and operate their weapons and financial resources than they did previously. In the previous parts of this study, how the internet-supported recruitment process works, which internet-based tools are used in this process, and which stage of the process should be given importance by the authorities to prevent the recruitment of terrorist organizations are described. This part discusses countermeasures to be implemented in the first stage of the internet-supported recruitment process, namely the earliest stage.

The use of the internet for terrorist purposes creates both challenges and opportunities for the defense against terrorism.[110] In the internet-supported recruitment process, while the internet is an ally to terrorist organizations that facilitates the process, they also unwittingly cooperate with their enemy.[111] The traditional recruitment process is an activity that is carried out confidentially and more securely in a specific geography and with a particular target audience. However, as analyzed in the second part of the study, anonymity and security are less in the first stage of the internet-supported recruitment process than in the traditional one and the second stage of the internet-supported recruitment process.[112] In that case, this is the stage where the authorities should focus on preventing recruitment efforts of terrorist organizations and the radicalization of vulnerable individuals.

In this regard, it is necessary to categorize the countermeasures taken by authorities to prevent terrorist organization recruitment. This study classified countermeasures to prevent terrorist organization recruitment efforts as active/hard and passive/soft. While active countermeasures aim to prevent terrorist organizations from obtaining human resources via internet-based technologies,

[110] United Nations, "The Use of The Internet for Terrorist Purposes," p. 3.

[111] Manuel R. Torres Soriano, "The Vulnerabilities of Online Terrorism," Studies in Conflict & Terrorism, 35 (2012), pp. 263-277, p. 264.

[112] Gabriel Weimann, "Terrorist Migration to Social Media," Georgetown Journal of International Affairs, 16 (1) (2015), pp. 180-187, p.185.

passive countermeasures aim to bridge the gap between vulnerable individuals, their families, and authorities. Furthermore, passive/soft countermeasures are intended to protect those exposed to terrorist recruiters' propaganda with the help of their efforts or the efforts of society and their relatives.

3.1. Active/Hard Countermeasures

Authorities aiming to prevent online radicalization and recruitment face some challenges because defining the recruitment process and radicalization "*online*" or describing it by adding the word "*online*" brings to mind the necessity of finding online solutions to prevent terrorist recruitment. There are many national and international countermeasures and practices to prevent terrorist organizations from recruiting new members, such as blocking online content and filtering/removing content that encourages radicalization.[113] However, many online platforms that facilitate communication and information sharing are operated by private companies. Moreover, each country has law enforcement regarding accessing and blocking online platforms.

Considering the convenience and freedom of access provided by today's internet technology, such countermeasures remain a temporary solution to prevent terrorist organizations from recruiting new members. Because blocked sites/user accounts can easily continue to exist on the internet with different IP addresses or user names.[114] According to a study conducted on 1000 pro-Daesh Facebook user accounts from 96 countries in 2018, it has been revealed that the organization's presence on this platform continues to grow despite the efforts to block and restrict these accounts. Furthermore, authorities may remain in an operational dilemma while taking these active/hard countermeasures. One side of this dilemma consists of the need for the protection of individuals, especially the young generation, who are inclined toward the ideology of terrorist organizations. On the other hand, the other side consists of controlled permission for these activities of the terrorist organization to gather intelligence about the recruitment efforts, propaganda tools, narratives, and target audience of terrorist organizations. It is impossible to hamper the recruitment process of terrorist organizations by just blocking their websites

[113] Zeiger et al., "Prevention of Radicalization on Social Media and the Internet," p. 359.

[114] Dodik Wirantoko and Bambang Wahyudi, "Counter Narrative Strategy of Terrorism Mitigation National Agency in Preventing Terrorism through Online Media," Journal of Strategic and Global Studies, 1 (1) (2018), pp. 47-58, p. 55.

and user accounts.[115] Therefore, authorities should balance this operational dilemma by implementing passive/soft countermeasures because it is not to be able to intervene in the recruitment process with active/hard measures alone to prevent the recruitment of terrorist organizations completely.

3.2. Passive/Soft Countermeasures

The blocking of websites, forums, blogs, and user accounts, as well as the arrest of those who run these platforms, is critical for preventing online radicalization. However, it is impossible to prevent terrorist organization recruitment completely with only these countermeasures, and passive/soft countermeasures should be integrated into them.[116]In this regard, building digital resilience and improving society's internet literacy are key points for preventing internet-supported recruitment of terrorist organizations. Passive/soft countermeasures should include the following practices to improve these abilities of society:

- Counter-narrative strategies,
- Positive message campaigns and,
- Training of vulnerable individuals, their families, and peers.

Terrorist organizations use narratives to promote violence and values contrary to human rights norms. They aim to exploit and radicalize vulnerable individuals to involve them in the cause.[117] In this regard, narratives are based on two approaches in the form of push or pull factors or their combination. While narratives focusing on pull factors consist of personal incentives, those focusing on push factors point out negative political, economic, and social issues that affect the living conditions of the target audience.[118] Terrorist organizations develop their narratives by using any of these approaches or a combination to establish a suitable environment for online recruitment since *"narratives are powerful resources for influencing target audiences.*[119]*"* For this reason, counter-narrative should not only include vulnerable

---

115 Freiburger et al., "A Systematic Explanation of Terrorist Use of the Internet," p. 317.

116 Wirantoko et al., "Counter Narrative Strategy of Terrorism Mitigation National Agency in Preventing Terrorism through Online Media," p. 47.

117 Jonathan Russel and Haras Rafiq, *Countering Islamist Extremist Narratives: A Strategic Briefing*, (Quilliam, 2016), p.3.

118 Zeiger et.al., "Prevention of Radicalization on Social Media and the Internet," p.361.

119 Steven R. Corman,"Understanding the Role of Narrative in Extremist Strategic Communication," in Countering Violent Extremism Scientific Methods & Strategies, (Laurie Fenstermacher and Todd Leventhal, eds, OH: Air Force Research Laboratory, 2011), pp. 36-43, p. 42.

individuals but also individuals on the path or already radicalized[120] because counter-narratives are not just counter-statements but messages that offer a positive alternative to terrorist propaganda.[121] Therefore, the original narrative should be identified, decrypted, and understood to fight against terrorist recruitment efforts. Moreover, authorities should examine the target audience's characteristics not only to produce better counter-narratives but also to capture the hearts and minds of vulnerable individuals.[122] Detection techniques and artificial intelligence can assist in identifying contents and narratives posted by terrorist organizations, and thereby authorities can have starting points for counter-narrative strategies.[123]

It can not be enough to hamper the recruitment of terrorist organizations with counter-narrative strategies created by the early detection and analysis of the narratives and propaganda materials of terrorist organizations. Especially the peers of the vulnerable younger generations can significantly contribute to the defense against terrorism. As discussed in the previous sections, the target audience of terrorism in the internet-supported recruitment process is the young generations who use online platforms the most. The most important reason for the terrorist organization to target this generation is to exploit their feelings, especially those foreign to their society, much easier. In other words, those unfamiliar with society cannot adequately establish a connection between the community and themselves due to the unaccepted attitudes of their peers and social environment. In that case, they can quickly become alienated from society. For this reason, it is essential to involve the peers of those inclined to terrorist ideology and alienated from society. In this regard, there are some good initiatives, such as *the Peer to Peer(P2P): Challenging Extremism Program* sponsored by U.S. federal agencies, including the Departments of Homeland Security and State, and *Peer to Peer (P2P): Facebook Global Digital Challenge*, which is a joint initiative with EdVenture

---

120 Michael Jacobson, "Learning Counter-Narrative Lessons from Cases of Terrorist Dropouts," in Counter Violent Extremist Narratives (National Coordinator for Counterterrorism, 2010), pp. 72-83, p. 75.

121 Henry Tuck and Tanya Silverman, *The Counter-Narrative Handbook,* (Institute for Strategic Dialogue, 2016), p. 4.

122 Amanda Langer, Marc-André Kaufhold, Elena M. Runft, Christian Reuter, Margarita Grinko, and Volkmar Pipek, "Counter Narratives in Social Media-An Empirical Study on Combat and Prevention of Terrorism," in Social Media in Crises and Conflicts Proceedings of the 16th ISCRAM Conference, (Zeno Franco, José J. González, and José H. Canós, eds., 2019), pp.746-755, p.747.

123 Langer et al., "Counter Narratives in Social Media-An Empirical Study on Combat and Prevention of Terrorism," p. 753.

Partners.[124] Such initiatives use a competitive model to engage student teams from universities worldwide to develop and implement social media campaigns to repel terrorist propaganda. They aim to create social media campaigns by engaging student teams from universities around the world to neutralize the narratives and propaganda of terrorist organizations. Such campaigns developed by students offer positive messages, promote tolerance and understanding of differences in society, and emphasize the possible contribution of diversity to society.[125]

The young generation can access unlimited and free information from anywhere, thanks to internet technology. They are exposed to different information content than those who are conventional media audiences because they were born into the computer-aided environment of the information era. Compared to previous generations, the young generation interacts with the internet almost daily, and their awareness of internet threats should be increased through training. In this regard, seminars, workshops, and even school-based lessons should be held to improve the young generation's internet literacy. Furthermore, this generation's families and relatives should be informed, and their support should be used to improve their children's awareness of internet-based threats. As a result, we should teach our children how to perceive various forms of information in developing technologies accurately and critically so that they can quickly identify disreputable websites and information resources.[126] In this way, internet literacy in the community can improve, which helps strengthen society's resilience to terrorist recruitment.

4. Conclusion

The opportunities provided by today's internet technology not only provide unprecedented benefits to terrorist organizations in terms of communication and recruitment but also leave them vulnerable to police monitoring because most of the activities of terrorist organizations over the internet are carried out through open sources. Authorities should focus on the initial stage of internet-supported recruitment, which is the most critical stage. Besides, they should take countermeasures to this recruitment process in combating human resources of terrorism since it has less confidentiality and is more open to police monitoring.

[124] See for detailed information at https://counterspeech.fb.com/en/initiatives/p2p-facebook-global/

[125] Szmania et al., "Countering Violent Extremism Online and Offline," p.2.

[126] John Curtis Amble, "Combating Terrorism in the New Media Environment," Studies in Conflict & Terrorism, 35 (5) (2012), pp. 339-353, p. 349-350.

Otherwise, after this stage, terrorist organizations take advantage of the confidentiality provided by internet technology to recruit new members and carry out their activities in areas where it is difficult for the authorities to detect. For this reason, the differences between the stages must be considered while developing countermeasures to render the recruitment process dysfunctional.

It is hard to combat the human resources of terrorist organizations just by blocking the websites or social media accounts by which terrorist organizations disseminate their narratives and propaganda. Moreover, legally arresting those who operate these websites/accounts is insufficient to hamper terrorist recruitment. As a result, authorities should combine hard countermeasures with soft ones comprehensively and effectively. In this context, while authorities can prevent terrorist organizations from operating their websites and social media accounts by practicing hard countermeasures, they also can take precautions against terrorist organizations' narratives and propaganda with soft countermeasures. In this way, authorities can raise awareness of the target audience and include the target audience's peers and relatives in the chain of countermeasures. Furthermore, increasing society's digital resilience against terrorist activities and improving internet literacy can significantly contribute to consolidating the chain of countermeasures. Figure-3 shows internet literacy and digital resilience that can be developed by integrating hard and soft countermeasures.

Consequently, the very early stage of the internet-supported recruitment process of terrorist organizations is examined in detail throughout the study. Although recruitment is a process and consists of stages, the first stage requires the most work and attention to combat the terrorist organizations' human resources. Because, as this study shows, after the first stage, terrorist organizations use internet technology to carry out their activities in complete secrecy. Therefore, it is hard to fight internet-supported recruitment of terrorist organizations only with hard countermeasures. In this regard, digital resilience against terrorism should be established, and the internet literacy of individuals should be improved to render the recruitment efforts of terrorist organizations dysfunctional.

Bibliography

Abdel R. Alzoubaidi, Doina Prodan-Palade, and Siddik Ekici, "Terrorist Recruitment and Counter Measures in the Cyber World," in Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operation, (Sıddık Ekici, Hüseyin Akdoğan, Eman Ragab, Ahmet Ekici and Richard Warnes, eds, IOS Press,2016), pp. 55-66.

Ahmet Sinan Yayla, Prevention of Recruitment to Terrorism, in Handbook of Terrorism Prevention and Preparedness (Alex P. Schmid ed., The Hauge, NL: ICCT Press, 2020), pp. 412-463, p.415.

Amanda Langer, Marc-André Kaufhold, Elena M. Runft, Christian Reuter, Margarita Grinko, and Volkmar Pipek, "Counter Narratives in Social Media - An Empirical Study on Combat and Prevention of Terrorism," in Social Media in Crises and Conflicts Proceedings of the 16th ISCRAM Conference, (Zeno Franco, José J. González, and José H. Canós, eds., 2019), pp.746-755.

Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," International Security, 31 (1) (2006), pp. 49-80.

Anna Stenersen, "The Internet: A Virtual Training Camp?" Terrorism and Political Violence, 20 (2) (2008), pp. 215-233.

Alex P. Schmid and Albert J. Jongman, et al., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases and Literature,* (Transaction Publishers, 1988).

Brian M. Jenkins, "International Terrorism The Other World War," (RAND Publication Series, A Project AIR FORCE Report Prepared for the United States Air Force, November 1985).

Bruce Hoffman, *Inside Terrorism,* (New York: Columbia University Press, 2006).

Çiğdem Erdin, "Radikal Selefi Örgütlerin Sosyal Medya Kullanımı: IŞİD Örneği," Bilge Uluslararası Sosyal Araştırmalar Dergisi, 1 (2) (2017), pp. 124-130.

Dodik Wirantoko and Bambang Wahyudi, "Counter Narrative Strategy of Terrorism Mitigation National Agency in Preventing Terrorism through Online Media," Journal of Strategic and Global Studies, 1 (1) (2018), pp. 47-58.

Dorothy E. Denning, *Terror's Web: How the Internet Is Transforming Terrorism,* in Handbook on Internet Crime (Yuonne Jewkes and Majid Yar eds., Willian Publishing, 2009).

Eddy Lynton J., Gerg Gullion, and James L. Williams, "Countering Terrorist Recruitment: Social Media, Cyber Terror, and Peaceful Platforms," in Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operation, (Sıddık Ekici, Hüseyin Akdoğan, Eman Ragab, Ahmet Ekici and Richard Warnes, eds, IOS Press, 2016), pp. 67-81.

Edgar Jones, "The Reception of Broadcast Terrorism: Recruitment and Radicalisation," International Review of Psychiatry, 29 (4) (2017), pp. 320-326.

Ergül Çeliksoy and Smith Ouma, "Terrorist Use of the Internet," Bilişim Hukuk Dergisi, 2 (2019), pp.243-267.

Ertan Efegil, *Terörizm ve Terörle Mücadele Yöntemleri,* (Gündoğan Yayınları, 2019).

European Commission's Expert Group on Violent Radicalisation, "Radicalisation Processes Leading to acts of Terrorism," (European Commission, 2008), available at https://www.clingendael.org/sites/ default/files/pdfs /20080500_cscp_report_vries.pdf (accessed May 3rd, 2022)

Gabriel Weimann, "How Modern Terrorism Uses the Internet," (United States Institute of Peace, Special Report, 2004).

Gabriel Weimann, "Cyber-Fatwas and Terrorism," Studies in Conflict & Terrorism, 34 (10) (2011), pp. 765-781.

Gabriel Weimann, "Terrorist Migration to Social Media," Georgetown Journal of International Affairs, 16 (1) (2015), pp. 180-187.

Gabriel Weimann, "The Emerging Role of Social Media in the Recruitment of Foreign Fighters," in Foreign Fighters under International Law and Beyond (Andrea de Guttry, Francesca Capone and Christophe Paulussen eds., T.M.C. Asser Press, 2016), pp. 77-95.

Gregory Waters and Robert Postings, "Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook" (Counter Extremism Project (CEP) Report, 2018).

Hasan D. Pekşen, "The Use of Media in the Transformation of Asymmetric Strategies: Common Logic, Different Methods," Güvenlik Bilimleri Dergisi, 10 (1) (2021), pp. 239-258.

Hayati Hazır, *Demokrasilerde İstikrarsızlığın Sebebi Olarak Siyasal Şiddet ve Terörizm* (Nobel Yayın Dağıtım, 2001).

Henry Tuck and Tanya Silverman, *The Counter-Narrative Handbook,* (Institute for Strategic Dialogue, 2016).

Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media," Social Science and Public Policy, 54 (2017), pp. 138-149.

James A. Lewis, "The Internet and Terrorism," Proceedings of American Society of International Law, 99 (2005), pp. 112-115.

John Curtis Amble, "Combating Terrorism in the New Media Environment," Studies in Conflict & Terrorism, 35 (5) (2012), pp. 339-353.

Jonathan Russel and Haras Rafiq, *Countering Islamist Extremist Narratives: A Strategic Briefing*, (Quilliam, 2016).

Ken Menkhause, "Al-Shabaab and Social Media: A Double-Edged Sword," Brown Journal of World Affairs, 20 (2) (2014), pp. 309-327.

Kaan Altınkaynak, "Sosyal Medyanın Kavramsal Çerçevesi ve Teknik Altyapısı," in Sosyal Medya Platformları (Mustafa Karaca ed., Anadolu University Press, 2019), pp. 3-15.

Logan Macnair and Richard Frank, "'To My Brothers in the West…': A Thematic Analysis of Videos Produced by the Islamic State's al-Hayat Media Center," Journal Contemporary Criminal Justice, 33 (3) (2017), pp. 234-253.

Manuel R. Torres Soriano, "The Vulnerabilities of Online Terrorism," Studies in Conflict & Terrorism, 35 (2012), pp. 263-277.

Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (University of Pennsylvania Press, 2008).

Mark Taylor, "An Analysis of Online Terrorist Recruiting and Propaganda Strategies," E-International Relations, available at https://www.e-ir.info/2017/07/19/an-analysis-of-online-terrorist-recruiting-and-propaganda-strategies/ (accessed January 9th, 2022).

Martin Rudner, "'Electronic Jihad': The Internet as Al Qaeda's Catalyst for Global Terror," Studies in Conflict & Terrorism, 40 (1) (2017), pp. 10-23.

Michael Jacobson, "Learning Counter-Narrative Lessons from Cases of Terrorist Dropouts" in Counter Violent Extremist Narratives (National Coordinator for Counterterrorism, 2010), pp. 72-83.

Mihaela Marcu, Cristina Bălteanu, "Social Media-A Real Source of Proliferation of International Terrorism," Annales Universitatis Apulensis Series Oeconomica, 16 (1) (2014), pp. 162-169.

North Atlantic Military Committee, "MC Concept for Counter-Terrorism (MC 0472/1, 2016)," available at https://www.nato.int/nato_static_fl2014/assets/pdf/topics_pdf/20160905_160905-mc-concept-ct.pdf (accessed April 20th, 2022).

Necdet Ekinci, "A Problem Growing in the Marsh Media: Terrorism," Karadeniz Sosyal Bilimler Dergisi, 8 (15) (2016), pp. 217-236.

Peter R. Neumann and Brooke Rogers, "Recruitment and Mobilisation for Islamist Militant Movement in Europe," (The International Centre for the Study of Radicalisation and Political Violence (ICSR) at King's College London for the European Commission (Directorate General Justice, Freedom, and Security)), pp. 49-53.

Peter R. Neumann, "The Trouble with Radicalization," International Affairs 89 (4) (2013), pp.873-893.

Sara Zeiger and Joseph Gyte, "Prevention of Radicalization on Social Media and the Internet," in Handbook of Terrorism Prevention and Preparedness (Alex P. Schmid ed., The Hauge, NL: ICCT Press, 2020), pp. 358-395.

Scott Gerwehr and Sara Daly, "Al-Qaida: Terrorist selection and Recruitment," (RAND Publication Series, 2006).

Sefer Darıcı and Ebru Karadoğan İsmayıl, "Popüler Kültür, Oyunlar ve Propaganda: Terörizmin Antropolojik Kodları," Bilge Strateji, 10 (19) (2018), pp. 39-65.

Shima D. Keene, "Terrorism and the Internet: a Double-edge Sword," Journal of Money Laundering Control, 14 (4) (2011), pp. 359-370.

Steven R. Corman, "Understanding the Role of Narrative in Extremist Strategic Communication," in Countering Violent Extremism Scientific Methods & Strategies, (Laurie Fenstermacher and Todd Leventhal, eds, OH: Air Force Research Laboratory, 2011), pp. 36-43.

Stuart Macdonald and David Mair, “Terrorism Online: A New Strategic Environment,” in Terrorism Online: Politics, Law and Technology (Thomas Chen, Lee Jarvis and Stuart Macdonald eds., Routledge, 2015).

Suzan Szmania and Phelix Fincher, “Countering Violent Extremism Online and Offline,” Criminology & Public Policy, 16 (1) (2017), pp. 119-125.

Tina Freiburger and Jeffrey S. Crane, “A Systematic Explanation of Terrorist Use of the Internet,” International Journal of Cyber Criminology 2 (1) (2008), pp. 309-319.

United Nations, “The Use of The Internet for Terrorist Purposes,” (United Nations Office on Drugs and Crime, 2012).

United Nations Counter-Terrorism Implementation Task Force, “Countering the Use of the Internet for Terrorist Purposes-Legal and Technical Aspects” (CTITF Publication Series, 2011).

Walter Laqueur, “Reflections on Terrorism,” Foreign Affairs, 65 (1) (1986), pp. 86-100.

William F. Shughart II, “Analytical History of Terrorism, 1945-2000”, Public Choice, 128 (1/2) (2006), pp. 7-39.

Vase Rusumanov, “The Use of Internet by Terrorist Organizations,” Information & Security: An International Journal, 34 (2) (2016), pp. 137-150.

Yusuf Devran, “The Problematics of Media and Terror,” Gumushane University E-Journal of Faculty of Communication, 3 (2015), pp.84-95.

Zakir Avşar, “Media, Terror and Security in the Age of Internet,” TRT Akademi, 2 (3) (2017), pp. 116-132.

Zsolt Haig and László Kovács, “New Way of Terrorism: Internet and Cyber-terrorism,” Aarms Security 6 (4) (2007), pp. 659-671.

“Foreign Jihadists in Syria: Tracking Recruitment Networks,” The Washington Institute for Near East Policy, available at https://www.washingtoninstitute.org/policy-analysis/foreign-jihadists-syria-tracking-recruitment-networks (accessed April 23rd, 2022).

“ISIL using Twitter App ‘Dawn’ to Keep Jihadists Update,” The Washington Times, available at https://www.washingtontimes.com/news/2014/jun/18/isil-using-twitter-app-dawn-keep-jihadists-updated/ (accessed April 24th, 2022).

“Up to 11,000 Foreign Fighters in Syria; Steep Rise among Western Europeans,” The Washington Institute for Near East Policy, available at https://www.washingtoninstitute.org/policy-analysis/11000-foreign-fighters-syria-steep-rise-among-western-europeans (accessed April 23rd, 2022).

https://counterspeech.fb.com/en/initiatives/p2p-facebook-global/

E-DATR, 2022; 16 : 69-108
ISSN 1307 - 9190

Lone-Actor Attacks and Organizational Connection: An Analysis of al Qaeda and Daesh Inspired Attacks in the European Union Zone

Tolga Ökten[1]

Abstract: *One of the main arguments in the terrorism studies literature is about the validity of the lone actors. While some studies defend that the definition of lone actor to be an oxymoron because it contradicts the generally accepted definition of terrorism, others argue that lone actors are very real. In this article, it is argued that lone actors have some distinct characteristics and that is why they are a real threat to European security. These features are theorized within the framework of the organizational connection variable, and the differences between lone actor and other organized attacks are examined. According to both statistical and descriptive analysis of these attacks, it is concluded that lone actor attacks are used as a conscious strategic choice by al Qaeda and Daesh leadership because of their unique characteristics.*

Keywords: *Lone Actors, Organizational Connection, al Qaeda, Daesh, European Union*

[1] Tolga ÖKTEN is an instructor of Intelligence Studies at the Turkish National Defence University. tolgaokten1982@gmail.com , ORCID: 0000-0002-6102-7704

1. Introduction

Al Qaeda- and Daesh-inspired terrorist attacks have become one of the top threat priorities for Europe in the first quarter of the 21st century.[2] These attacks have different characteristics within the framework of organizational connection. In particular, a certain number of attacks were committed by aggressors without direct organization linkage. This situation has led to discord among researchers about the role of lone actors in the attrition strategy of al Qaeda and Daesh. While some researchers argue for the validity of lone actors, others argue that no actor is truly alone.[3]

Lone-actor studies are an important research topic in the terrorism literature. The interest of the academic community and the security bureaucracy in the concept of the lone actor has rapidly increased since the beginning of the 2000s. Conflicts in Afghanistan, Iraq, Syria, and Libya have been spread in Europe and the USA in the form of terrorist attacks, and lone actors have become one of the prominent threat scenarios. Due to the frequent utilization of this type of attack, the attention of researchers has also incrementally increased throughout the 21st century. According to one study, between 2009 and 2012, an average of 300 articles began to be published every year in major sources in English, and this number exceeded 1000 in 2016.[4] These studies examine dimensions such as: motive,[5] demographic features,[6] the role of mental illness,[7]

---

2 According to the Global Terrorism Database, a total of 872 people were killed in Al-Qaeda and Daesh perpetrated/inspired terrorist attacks between 2001-2017 in Europe.

3 This debate is detailed in the fourth part of the article.

4 Jason Burke, "The Myth of the 'Lone Wolf' Terrorist", *The Guardian*, (30 March 2017), available at https://www.theguardian.com/news/2017/mar/30/myth-lone-wolf-terrorist#img-4 (Accessed 03 March 2021)

5 Jeffrey Kaplan, Helene Lööw and Leena Malkki, "Introduction to the Special Issue on Lone Wolf and Autonomous Cell Terrorism", *Terrorism and Political Violence* 26(1) (2014), pp.1-12; Matthew Feldman, "Comparative Lone Wolf Terrorism: Toward a Heuristic Definition", *Democracy and Security* 9(3) (2013), pp.270-286; Jeff Gruenewald, Steven Freilich, Joshua Chermak, "Distinguishing 'Loner' Attacks from Other Domestic Extremist Violence A Comparison of Far-Right Homicide Incident and Offender Characteristics", *American Society of Criminology Criminology & Public Policy* 12(1) (2013), pp.65-91; Randy Borum, "Loner Attacks and Domestic Extremism Informing Lone-Offender Investigations", *Criminology & Public Policy*, 12(1) (2013), pp.103-112; Sarah Teich, "Trends and Developments in Lone Wolf Terrorism in the Western World an Analysis of Terrorist Attacks and Attempted Attacks" (IDC Herzliya International Institute of Counter Terrorism October 2013).

6 Clark Mccauley, Sophia Moskalenko and Benjamin Van Son, "Characteristics of Lone-Wolf Violent Offenders: A Comparison of Assassins and School Attackers", *Perspectives on Terrorism* 7(1) (2013), pp.4-24; Paul Gill, John Horgan and Paige Deckert, "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists" *Journal of Forensic Sciences* 59(2) (2014), pp.425-435.

7 Emily Corner, Paul Gill, and Oliver Mason, "Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence" *Studies in Conflict & Terrorism* 39(6) (2016), pp.560-568.

modus operandi,[8] target selection,[9] terrorism–crime nexus[10] and organizational connection.[11] They aim to conceptualize this phenomenon by creating various typologies and determine the common characteristics of lone actors.[12] Many of these studies are empirical. Some of them use small-N analysis on selected cases;[13] others try to determine common lone-actor characteristics using large-N analysis.[14] The terminology of the lone-actor phenomenon also differs among these

8 Ramon Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment" *Studies in Conflict & Terrorism* 33(9) (2010), pp.854-870; Petter Nesser, "Single Actor Terrorism: Scope, Characteristics and Explanations", *Perspectives on Terrorism* 6(6) (2012), pp.61-73.

9 Zoe Marchment, Noémie Bouhana and Paul Gill, "Lone Actor Terrorists: A Residence-to-Crime Approach", *Terrorism and Political Violence*, 32(7) (2018), pp.1-16.

10 Rajan Basra, Peter Neumann and Claudia Brunner, "Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus, The International Centre for the Study of Radicalisation and Political Violence (ICSR) 2016).

11 Peter Phillips, Gabriela Pohl, "Economic Profiling of the Lone Wolf Terrorist: Can Economics Provide Behavioral Investigative Advice?", *Journal of Applied Security*, 7(2) (2012), pp.151-177, p.174. Rodger Bates, "Dancing with Wolves: Today's Lone Wolf Terrorists", *The Journal of Public and Professional Sociology*, 4(1) (2012), pp.1-14., p.8-9; Raffaello Pantucci, "Developments in Radicalisation and Political Violence A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists", (King's College International Centre for the Study of Radicalisation and Political Violence 2011), p.14.; "The Threat From Solo Terrorism and Lone Wolf Terrorism", (Politiets Efterretningstjeneste Center For Terroranalyse 2011), p.3; Randy Borum, Robert Fein and Bryan Vossekuil, "A Dimensional Approach to Analyzing Lone Offender Terrorism", *Aggression and Violent Behavior*, 17(5) (2012), pp.389–396, p.389-396;
Sebastien Feve, Kelsey Bjornsgaard, "Countering Lone-Actor Terrorism Series No. 3", (Royal United Services Institute for Defence and Security Studies Lone-Actor Terrorism Database Workshop 2016).; Bart Schuurman, Edwin Bakker, Paul Gill, and Noemie Bouhana, "Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis", *Journal Forensic Sciences*, 63(1) (2017), pp.1191-1200; Caitlin Clemmow, Noémie, Bouhana and Paul Gill, "Analyzing Person-Exposure Patterns in Lone-Actor Terrorism", *Criminology & Public Policy*, 19(2) (2019), pp.1-31.

12 The Terrorist Radicalization Assessment Protocol-18 / TRAP-18, developed by the Global Institute of Forensic Research to create a common lone actor typology, also has an important place in the current literature. See J. Reid Meloy, Paul Gill, "The Lone-Actor Terrorist and the TRAP-18", *Journal of Threat Assessment and Management*, 3(1) (2016), pp.37–52, p.39.

13 David Hofmann, "How 'Alone' are Lone-Actors? Exploring the Ideological, Signaling, and Support Networks of Lone-Actor Terrorists, *Studies in Conflict & Terrorism*, 43(7) (2018), p.7; Thomas Holt, Joshua Freilich, Steven Chermak, Colleen Mills and Jason Silva, "Loners, Colleagues, or Peers_ Assessing the Social Organization of Radicalization", *American Journal of Criminal Justice*, 22(1) 2018, pp.83-105; Petter Nesser, Anne Stenersen and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect", *Perspectives on Terrorism*, 10(6) (2016), pp.3-24.

14 Brent Smith, Jeff Gruenewald, Paxton Roberts and Kelly Damphousse, "The Emergence of Lone Wolf Terrorism: Patterns of Behaviour and Implications for Intervention", *Sociology of Crime, Law and Deviance*, 20 (2015), pp.89–110; Mark Hamm, Ramon Spaaij, "Lone wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies", (U.S. Department of Justice 2015); Jeff Gruenewald, William Pridemore, "A Comparison Of Ideologically-Motivated Homicides from the New Extremist Crime Database and Homicides from the Supplementary Homicide Reports Using Multiple Imputation by Chained Equations to Handle Missing Values", *Journal of Quantitative Criminology*, 28(1) (2012), pp.141-162; Clare Ellis, Raffaello Pantucci, Jeanine de Roy van Zuijdewijn, Edwin Bakker, Benoît Gomis, Simon Palombi and Melanie Smith, "Lone-Actor Terrorism: Analysis Paper" (Royal United Services Institute 2016).; John Horgan, Paul Gill, Noemie Bouhana, James Silver and Emily Corner, "Across the universe? A Comparative Analysis of Violent Behavior and Radicalization Across Three Offender Types with Implications for Criminal Justice Training and Education", (National Institute of Justice 2016); Gill, et. al. Ibid.; Schuurman et. al., Ibid.

studies. Due to its adoption by the media, the most popular usage is the term lone wolf. On the other hand, there is a general opinion that the term lone wolf should not be used because of its honorific connotation. Suggested alternatives include lone actor",[15] lone offender,[16] and terrorists acting alone.[17] In this study, the term lone actor is used.

This article's main research topic is the organizational connection of al Qaeda- and Daesh-related attacks. The purpose is to explore whether the attacks carried out by al Qaeda and Daesh can be classified as lone-actor attacks. The hypothesis is that some of these attacks were committed under organizational isolation (ideological and operational) and that is why they can be classified as lone-actor attacks. These isolated attacks differ dramatically from other high-profile organized suicide attacks not only in the variable of organizational connection but also in the dimensions of legal status, tactics, and mental health. Due to these unique characteristics, lone actors manage to paralyze security bureaucracy on many occasions. To operationalize this hypothesis, the data of EUROPOL's Annual European Union Terrorism Situation and Trend Reports are used.[18] That is why the study is limited by the European Union zone. The methodology is based on large-N analysis and the interpretation of statistical data.

The article consists of four main parts. In the next part, the strategic logic of lone-actor attacks is explained. In this manner, the importance of lone actors in terrorism studies and why these isolated attackers create an important global security threat is also stated. In the third part, the role of lone actors in the strategy of al Qaeda and Daesh is examined. Accordingly, historical background of these attacks is investigated. In the fourth part, the theoretical framework of organizational connection is constituted and the difference between narrow and broad conceptualizations is explained. In the last part, the al Qaeda- and Daesh-related attacks in the European Union zone are analyzed and the findings are discussed. The findings are concentrated on the mental illness, crime nexus, legal statuses, target choices, and tactics.

15 "Joint Publication 3-26 Counterterrorism", (U.S. Army 2009); Edwin Bakker, Jeanine de Roy van Zuijdewijn, "Countering Lone-Actor Terrorism Series No. 2.", (Royal United Services Institute for Defence and Security Studies Lone-Actor Terrorism Definitional Workshop 2015).

16 https://www.fbi.gov/investigate/terrorism

17 "Bringing Terrorists to Justice: Challenges in the Prosecution of Terrorists Acting Alone or in Small Cells", (United Nations 2015). https://www.un.org/sc/ctc/wp-content/uploads/2015/09/S_2015_123_EN.pdf.% (Accessed 03 October 2020)

18 The annual European Union Terrorism Situation & Trend Reports can be accessed from EUROPOL's web site. https://www.europol.europa.eu/publications-events/main-reports/tesat-report

2. The Strategic Logic of Lone Actor Attacks

Lone-actor attacks are not just about tactical choices. As these attacks are remotely inspired and sometimes directed by the leadership cadre of terrorist organizations, it is also a strategic choice for terrorist organizations. The main aim of these attacks is to utilize difficulties experienced by intelligence units in detecting the attackers, who do not establish organizational contact at the ideological and operational levels. Lone actors have a high level of operational security against penetrations and therefore became an effective option for terrorist organizations. Besides, by using the lone actors, terrorist organizations such as al Qaeda and Daesh extended their activities beyond conflict zones.

On the other hand, lone-actor attacks are more improvised, and simpler, since they are usually handled by people who do not have sufficient technical-tactical experience and logistics. In fact, this is a profit and loss balance. The limited experience and logistics are one of the main sources of operational security. Lone actors, who do not enter the organizational hierarchy and go directly to the action phase, leave very small footprints behind them and are able to bypass preventive measures of security and intelligence agencies. Even after the attack, it may not be possible to determine whether the attacker has any organizational connection or not.

It can be said that the lone actors are attackers who commit crimes on behalf of the organization, although they are not legally members of the organization. Although their victims are random and that is why their motivation is political, there is not any significant organizational connection with a terrorist group. They radicalize and become operational without any physical contact from overseas. Unlike traditional organizational structures, the operational process develops from the bottom up, not from the top down. Operational directions are given by organizational ideologists and media organizations using open sources. Due to the high level of exposure, it is not possible to determine who has become operational by taking these instructions seriously. For this reason, although there were signs of radicalization in many examples, legal action could not be carried out.

The most important task of intelligence agencies is warning against attacks. They can do this by exploiting their technical and human assets in a terrorist organization. Lone actors have the potential to paralyze this sequence. Due to the minimum level of organizational engagement, lone actors do not give signals before attacking. Even if there are signals, they are lost in the noise. Because of this weak link, it is assumed that it is impossible to prevent them

completely.[19] There are even views stating that security forces should focus on preventing more organized and dangerous attacks, such as the 9/11 attacks, rather than those perpetrated by these isolated actors.[20]

The low signal-to-noise ratio is also emphasized by the authorities. Chief of General Staff of the Israel Defense Forces General Gadi Eizencott stressed that, *"there were no warnings about suicide stabbing attacks. Israel faced 101 such events in the past three months, but we did not have even one single warning".*[21] In his statement to the Senate Intelligence Committee in 2010, CIA Director Leon Panetta said, *"The biggest threat is not so much that we face an attack like 9/11. It is that al Qaeda is adapting its methods in ways that oftentimes make it difficult to detect… it's the lone-wolf strategy that I think we have to pay attention to as the main threat to this country".*[22] FBI Director Robert Mueller, in his statement to the Intelligence Committee in 2003, stated that the actions of lone actors are very difficult to predict and therefore form a major security threat.[23] The threat posed by lone-actor terrorism is also revealed by MI5 President Andrew Parker. While responding to the criticisms about the inability to prevent attacks such as Parker, Westminster, Manchester, and London Bridge, he said, *"that threat (lone actors) is multi-dimensional, evolving rapidly and operating at a scale and pace we've not seen before…It's at the highest tempo I have seen in my 34-year career. Today there is more terrorist activity, coming at us more quickly, and it can be harder to detect."*[24] It is also emphasized that MI5 was tracking approximately 3000 radicals in 2017 as terror suspects.[25]

---

19 Spaaij, ,Ibid, p.867.; Edwin Bakker, Beatrice de Graaf, "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed", *Perspectives on Terrorism*, 5(5-6) (2011), pp.43-50; Brian Jenkins, "Stray Dogs and Virtual Armies Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11", (RAND 2011); PET CTA, ibid, p.3.

20 Beau Barnes, "Confronting the one-man Wolf Pack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism", *Boston University Law Review*, (92) (2012), pp.1613-1662.

21 Gili Cohen, "Eizencott: Out of 101 Knives Attacks We Did Not Have Even One Warning," Haaretz (18 January 2016), http://www.haaretz.co.il/news/ politics/1.2824704 (Hebrew) cited in Avner Barnea, "Challenging the 'Lone Wolf' Phenomenon in an Era of Information Overload", *International Journal of Intelligence and Counterintelligence*, 31(2) (2018), pp.217-234, p.221

22 "CIA Chief: Al Qaeda Poised to Attack U.S.", CBS (2010) available at https://www.cbsnews.com/news/cia-chief-al-qaeda-poised-to-attack-us/. (accessed 05 June 2020).

23 Robert Mueller, "War on Terrorism", (Testimony before the Select Committee on Intelligence of the United States Senate 2003), available at https://archives.fbi.gov/archives/news/testimony/war-on-terrorism (accessed 12 November 2020).

24 "UK Facing Most Severe Terror Threat Ever, Warns MI5 Chief", *The Guardian*, available at https://www.theguardian.com/uk-news/2017/oct/17/uk-most-severe-terror-threat-ever-mi5-islamist (Accessed 05 July 2021).

25 "A Former MI5 Agent Tells us Why it's so Easy for Terror Suspects like Khalid Masood to Move Around without Being Arrested", *Business Insider*, available at http://uk.businessinsider.com/mi5-agent-surveillance-of-islamic-terrorist-suspects-2017-3 (Accessed in 12 November 2020).

Due to the sudden nature of attacks they should be followed 24/7, and it is an impossible task.

Even if a signal is detected, it is not easy to convict a potential attacker. This situation poses a great problem for countries with democratic systems. Security agencies have difficulties in detecting the transition from the phase of speech, which is accepted as freedom of expression, to the phase of action. It is not possible to detect the exact time at which actors move from speech to action, to follow all radicals, and to protect all possible targets. Moreover, in the criminal justice system, a criminal organization must operate under a hierarchical structure and there must be continuity in its activity. Weapons and logistics are required to commit the crime. If these conditions are not met, the issue is legally seen as a preparatory action and cannot be punished.[26]

Moreover, in some occasions, a potential lone actor cannot take action due to insufficient capacity in terms of logistics. It is known that these actors are radicalized, but legal steps cannot be taken because an operational link cannot be proved. In such cases, security forces have three different options. In the first option, these radicals are generally put into technical and physical surveillance. However, this does not guarantee the prevention of an attack.[27] Another method is internment, but in democratic countries, it is not always legally possible to intern all of the potential attackers. Even if this is done, it may not be efficient. Taking advantage of the state of emergency, in France, a total of 3600 operations were carried out without a court decision between November 2015 and July 2016, but only one suspect was prosecuted.[28] The last option is the sting operation. In this

---

[26] Zeki Hafızoğulları, Günal Kurşun, "Türk Ceza Hukukunda Örgütlü Suçluluk", *TBB Dergisi*, (71) (2007), pp.25-80, p.39. (in Turkish)

[27] For example, Khamzat Azimov, a radical who was under control of the French police forces, stabbed a person to death on 12 May 2018 in Paris. See "Paris Knife Attacker was Known to Counter-Terrorism Police", (13 May 2018), *The Guardian*, available at https://www.theguardian.com/world/2018/may/13/paris-knife-attacker-khamzat-azimov-known-to-counter-terrorism-police (Accessed 08 October 2020).

[28] Martin de Bourmont, M., "Rights Advocates Brace for Anti-Terrorism Bill", *Foreign Policy*. (03 October 2017); Authorities say that going to Afghanistan or praising al Qaeda and Daesh will put a person on the FBI's radar, but not enough to be charged and arrested. For example, Omar Mateen, who killed 49 people in an attack on a nightclub in Orlando on June 12, 2016, had been interrogated and placed under surveillance before the attack, because of making radical rhetoric at work. FBI Director of the time, Comey, stated that the FBI conducted a preliminary investigation against Mateen for 10 months, which is the legal limit, but no signs of a threat were found, and in hindsight, no action was incomplete or wrong in this case and that they should have done differently. Adam Goldman, "Why Didn't the F.B.I. Stop the New York Bombing?" (21 September 2016). Available at https://www.nytimes.com/2016/09/22/us/fbi-terror-ahmad-khan-rahami.html (Accessed 10 October 2020).

scenario, a potential attacker passes to the action phase and is removed from the system under the control of the intelligence agencies. In the USA, between 2001-2013, a total of 15 potential lone actors (25% of lone actor cases in the USA) were prosecuted in this way.[29] Although sting operations are very successful at the tactical level, it brings moral discussions with it. For this reason, it is not preferred in European Union countries.

As previously mentioned, lone actors have the ability to put intelligence and security agencies on the horns of a dilemma due to their unique character. For this reason, these kinds of attacks are also preferred by al Qaeda and Daesh. In the next part, the background of these organizations lone actor campaigns is examined.

3. The Lone Actors in the Strategy of al Qaeda and Daesh

Lone-actor attacks are not a new phenomenon. Although some researchers indicates that the concept of an actor acting alone has always been an important figure throughout the human history,[30] the modern era of lone actors is generally initiated by the assassination campaign of 19th century anarchists. In this era, anarchists carried out assassinations and attacks against institutions and individuals representing bourgeois values and monarchies, in the form of small cells or individuals. That is why the period of 1878–1934, when anarchists carried out serial assassinations, is seen as the classical age of lone actors.[31] The concept of "propaganda by the deed", the famous slogan of the period, triggered such actions.[32]

The concept of lone actor became popular in the USA after being placed in a theoretical framework under the concept of *"leaderless resistance"* by right-wing domestic terrorist organizations in the U.S. The definition has its origins in an article of the same title, dated 17 April 1962 by Captain Ulius Louis Amoss.[33] It was formulated as an *"irregular warfare against invading communist troops"*.[34] Ironically, the model was applied by the US far right against the US federal government in the last quarter of the 20th century.[35] The concept's popularity increased in

[29] Ramon Spaaij, Mark Hamm, "Key Issues and Research Agendas in Lone Wolf Terrorism", *Studies in Conflict & Terrorism*, 38(3) (2015), pp.67-178, p.172.

[30] Bates, Ibid, p.2; Kaplan, et., Ibid, p.1.

[31] Richard Jensen, "The Pre-1914 Anarchist 'Lone Wolf' Terrorist and Governmental Responses", *Terrorism and Political Violence*, 26(1) (2014), pp.86-94, p.87; Feldman, Ibid, p.272-273.

[32] Borum et. al., p.389.

[33] Louis Beam, "Leaderless Resistance", *The Seditionist,* (12 February 1992), available at http://www.louisbeam.com/leaderless.htm. (Accessed 10 May 2020).

[34] Jeffrey Kaplan, "Leaderless Resistance", *Terrorism and Political Violence,* 9(3) (1997), pp.80-95, p.80

[35] Kaplan, Ibid, pp.80-87.

1983, when Louis R. Beam, a former Ku Klux Klan and Arian Nations member, once again brought it into the agenda. Beam, due to being influenced by Amoss, used the definition of *"leaderless resistance"* and conceptualized it as "*lone wolf*" actions carried out individually or by a small group, independent of any network or movement. Beam stated that the pyramid-shaped, hierarchical structure has proven to be unsuccessful against the state apparatus. An alternative to pyramid structuring was a cell-type organization. Beam emphasizes that the cell structure, which he calls the *"communist model"*, has a centralized organization, direction, and financing, but *"American patriots"* do not have such opportunities. Beam states that the third option, other than the pyramid and cell structure, is what Amoss refers to as the *"phantom cell"*. Although this system is a cell structure, it is not connected to a center, and all individuals and groups connected to the movement act independently. Instructions are given over media without direct contact with cells. [36]

Lone-actor attacks also have an important place in al Qaeda narratives. Al Qaeda defines lone actors as individuals who act outside the chain of command; the origins of this methodology can be traced back to the book The Call to Global Islamic Resistance, written by Mustafa bin Abd al-Qadir Setmariam Nasar aka Abu Musab al-Suri in the 1990s.[37] This publication is considered to have been instrumental in al Qaeda's turn to lone-actor attacks in 2004. In his book, al-Suri defined lone actors as individuals or small cells who keep their ties to the organization to a minimum. In this way, intelligence units will be confused and the discovery of a cell will not pose a threat to other cells.[38] Al Suri places lone-actor attacks at the center of his modus operandi. He emphasizes that, instead of a guerrilla type of warfare based on armed groups, small cells or "individual jihad" should be waged in regions where it is not possible to open a front.[39] This doctrine was expressed as *"nizam, la tanzim"* (system, not organization). Accordingly, there is no need for any operational link to take action, and guidance will be sufficient. [40]

---

36 Beam, Ibid.

37 Rachel Briggs, "The Changing Face of al Qaeda", (Institute for Strategic Dialogue January 2012).

38 Gabriel Weimann, "Lone Wolves in Cyberspace", *The Centre for the Study of Terrorism and Political Violence*, 3(2) (2012), pp.75-90, p.82.

39 (PET CTA, Ibid., From Brynjar Lia, "Al-Suri's Doctrines for Decentralized Jihadi Training – Part 1", *Terrorism Monitor*, 5(1) (2007), available at https://jamestown.org/analyst/brynjar-lia/ (Accessed 15 May 2020).

40 Lia, 2007; Al Suri gave importance not only to the lone actor attacks but also to more sophisticated terrorist attacks that required detailed planning such as the 2004 Madrid and 2005 London bombings. See "Syria Releases the 7/7 Mastermind", *The Telegraph* (04 February 2012), available at https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9061400/Syria-releases-the-77-mastermind.html, (Accessed 20 May 2020).

Lone-actor attacks have been promoted by al Qaeda leadership. In an article published on a website called Sada al Jihad by Osama bin Laden in 2003, he called for action without waiting for any instructions.[41] This concept was indoctrinated in a series of articles titled "How to Fight Alone", published in 2006 by al Qaeda member Abu Jihad al-Masri.[42] Al Qaeda leader Ayman al-Zawahiri, in his message on September 11, 2013, the 12th anniversary of 9/11, praised the Boston Marathon attack and stated that similar attacks should be carried out by lone actors or small cells. Zawahiri also emphasizes that the most important effect of lone actor threat is in the economic dimension and that the threat of attack will lead the US to increase its security expenditures and to live under the constant fear of an attack. He states that these attacks do not have any cost for al Qaeda, but they bring a great burden to the US economy.[43]

Lone-actor attacks have also been embraced by al Qaeda affiliates like al Qaeda in the Arabian Peninsula (AQAP). In fact, in the first decade of the 21st century, the most active affiliate of al Qaeda was AQAP and Ibrahim al-Asiri, the group's explosives expert, who was described by David Petraeus, the head of the CIA at the time, as *"the most dangerous man in the world"*.[44] It is believed that AQAP had an ideological or operational role in many actions carried out in Europe and the USA between 2009 and 2016.[45] The pivot in AQAP's lone-actor attacks was al-Awlaki. As a US citizen, al-Awlaki has been a mentor and a role model for radicals in the US. Besides, in Inspire, the media branch of the organization, lone-actor style improvised attacks were encouraged with articles such as "Make a Bomb in the Kitchen of Your Mom". These articles guided attackers like Tsarnaev brothers.[46]

Al Qaeda in Iraq (AQI - later Daesh) was another affiliate that prioritized lone actors in their strategy. Daesh's turn to lone-actor attacks is the direct result of its failures in the conflict zones. In this context, there has been a great increase in calls for attacks against Western targets, especially after 2014. Hamming states that, while the leadership cadre of Daesh called for an attack against Western targets (far enemy) only once between 2010-2014, this number dramatically increased to

---

41 Borum, et. al., p.391.

42 Borum, et. al., p.391.

43 "Al-Qaeda Chief Zawahiri Urges 'Lone-Wolf' Attacks on U.S.", *BBC*, (13 September 2013, https://www.bbc.com/news/world-middle-east-24083314 (accessed 20 October 2021).

44 Interview with Peter Bergen in "David Petraeus: ISIS is on its Way to Defeat but Terrorism Threat Persists", *CNN*, available at https://edition.cnn.com/2016/06/22/opinions/bergen-interview-with-petraeus/index.htm, (Accessed 20 October 2021)

45 Colin Clarke, "Predicting the Next ISIS", (08 October (2018), available at https://nationalinterest.org/feature/predicting-next-isis-32822 (accessed 24 May 2020)

46 Jesse Morton, Mitchell Silber, "NYPD vs. Revolution Muslim: The Inside Story of the Defeat of a Local Radicalization Hub", *CTC Sentinel*, 11(4) (2018), p.5.

11 between 2014-2018.[47] Daesh's first statement targeting Europe was given in September 2014 by the organization's spokesman and the leader of the foreign operations unit Emni[48], Abu Muhammad al-Adnani. The statement came seven days after the announcement of the international coalition against Daesh.[49] In the statement Adnani called for retaliatory attacks against civilian and military targets in the West. In this call, Adnani encouraged potential lone actors to improvised attacks and said *"If you are not able to find… a bullet, then … [s]mash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him".*[50] In another speech in May 2016 he said, *"the smallest action you do in their heartland is better and more enduring to us than what you would [do] if you were with us…we wish we were in your place to punish the Crusaders day and night"*.[51]

Accordingly, since 2014, the main body behind most of the terrorist attacks in Europe is the Emni organization, the foreign operations unit of Daesh. Emni both organized and inspired terrorist attacks and, like AQAP's terror campaign between 2009 and 2015, it carried out a brutal campaign in Europe between 2015 and 2016.[52] The organization was established in 2014 and initially operated from Al Bab in Syria until 2016. After Emni's removal from al Bab by the Turkish Armed Forces, its headquarters was moved to Libya. Since his ties with Libya date back to 2016, this departure was not a spontaneous move. It is known that the cadres of Katibat Al-Battar Al-Libi (KBL), a local Libyan group, served as autonomous cells within Daesh in Syria.[53] The cooperation between Emni and KBL has created a dangerous outcome for Europe; besides remotely inspired lone-actor attacks, more complicated and centrally planned attacks have also been initiated by this group. There were two main drives behind this outcome. First of all, KTB enabled

---

47 Tore Hamming, "Jihadi Competition and Political Preferences", *Perspectives on Terrorism*, 11(6) (2017), pp.63-88; In this context, the first Daesh inspired lone actor attack was carried out by Amedy Coulibaly in Paris in January 2015. Mona Alami, "Parsing the Islamic State's Nice Attack Claims" (19 July 2016) available at http://www.atlanticcouncil.org/blogs/ menasource/parsing-the-islamic-state-s-nice-attack-claims, (accessed 11 May 2020)

48 Can be translated as "security".

49 Nesser et. Ibid, p.5.

50 Abu Muhammad Al-Adnani, "Indeed Your Lord Is Ever Watchful", (9 September 2014) cited in Basra et. al., Ibid, p.35.

51 Abu Muhammad Al-Adnani, (May 2016), cited in Maher Chmaytelli and Stephen Kalin and Ali Abdelaty "Islamic State Calls for Attacks on the West during Ramadan in Audio Message", *Reuters*, available at https://www.reuters.com/article/us-mideast-crisis-islamicstate-idUSKCN0YC0OG, (accessed 15 June 2021).

52 Clarke, Ibid.

53 Jacqueline Sutherland, "How Is ISIS Able to Commit Acts of Terror as It Loses Territory?", (08 November 2017), *The National Interest*, available at https://nationalinterest.org/feature/how-isis-able-commit-acts-terror-it-loses-territory-23111 (accessed 15 June 2021)

Emni to reach Western European radicals. These radicals were Francophone cadres from Belgium, France, and Tunisia that had previously operated within the KTB. It is considered that linguistic proximity may be effective in this. The second reason was about the tactics. It is argued that the *inghimasi* tactics, which combine armed assault and suicide bombing, were popularized by the KTB. In this context, it is said that the attacks carried out by French and Belgian cadres in Europe with *inghimasi* tactics possibly had been directed by the KTB.[54]

4. The Lone Actor Conceptualizations and the Theoretical Framework

The conceptualizations in the literature can be divided into two groups, narrow and broad, within the framework of the organizational-link variable. The main points that separate these two groups are the ideological[55] and operational ties of the attackers. Researchers that use the narrow definition oppose all kinds of ideological and operational connection. Other studies using the broad definition agree that there may be an ideological relationship but they differ on the operational connection (Figure-1). Since fundamentalist organizations like al Qaeda started to exploit the lone actor attacks, there has been an inclination to use a broader definition.

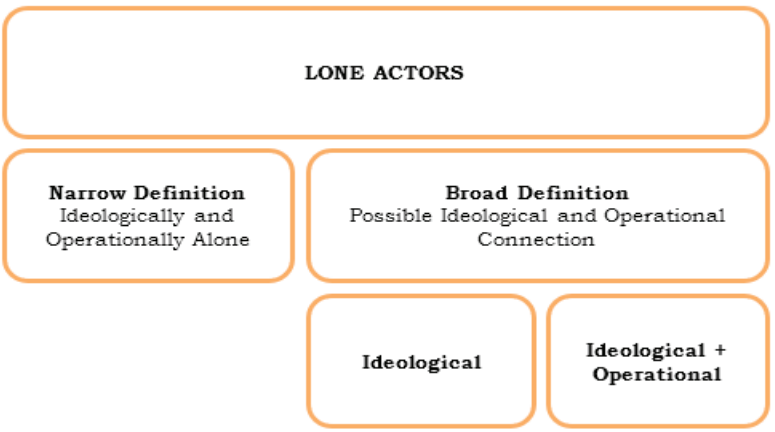


Figure 1: Narrow and Broad Definitions[56]

[54] Cameron Colquhoun, "Tip of the Spear? Meet ISIS' Special Operations Unit, Katibat al-Battar", (16 February 2016), *Bellingcat*, available at https://www.bellingcat.com/news/mena/2016/02/16/tip-of-the-spear-meet-isis-special-operations-unit-katibat-al-battar, (accessed 15 June 2021).

[55] Clearly all al Qaeda and Daesh inspired attackers are ideologically motivated. In this research, the ideological connection variable is used to describe whether the attackers have made any organizational connection in their radicalization process.

[56] The figure was prepared by the author.

4.1. Narrow Conceptualization

The narrow conceptualization emphasizes that the aggressor must act completely alone during the radicalization process, operational preparation phase, and at the moment of action. Accordingly, if the attacker establishes an organizational connection at the operational level or a cell formation occurs, the lone-actor characteristics are lost. Any kind of an organizational connection is against the secrecy inherent to the definition of the lone actor.[57] Therefore, attackers that come into contact with radical circles in virtual or physical environments do not fall within the narrow definition of the lone actor. [58]

Since terrorism is generally accepted as an organized crime with political aims, it is difficult to come across an attacker who fits this narrow definition. Accordingly, the narrow conceptualization is largely inherent to office-campus attackers and serial killers who act for personal reasons. In this context, the narrow definition excludes many aggressors who are defined as lone actors in popular opinion. For example, Breivik is not considered a lone actor because he is ideologically linked to far-right groups.[59] A similar situation applies to McVeigh too.[60]

The most popular example (maybe the only according to narrow definition) that falls within the narrow conceptualization is Theodore Kaczynski, aka the UNABOMBER (University and Airline Bomber), who acted completely alone ideologically and operationally. Kaczynski, an American mathematician and anarchist, caused the death of 3 people and the injury of 23 people in 16 separate bomb attacks, which he carried out for 17 years. He claimed that technology was destroying the social structure and that is why he targeted scientists who were engaged in technological research. Kaczynski also unsuccessfully tried to shoot down a domestic flight in the USA in 1979. Due to his organizational isolation, he managed to hide from the radar of intelligence units for many years.

---

57 Bakker, Zuijdewijn, Ibid, p.6.

58 J.M. Berger, "The Boy Who Cried Lone Wolf", (12 February 2012), *Foreign Policy*, available at https://foreignpolicy.com/2012/02/21/the-boy-who-cried-lone-wolf/. (accessed 10 June 2020); Fred Burton, Scott Stewart, "The 'Lone Wolf' Disconnect", (30 January 2008), *The Stratfor*, available at www.stratfor.com/weekly/lone_wolf_disconnect, (accessed 10 May 2020).

59 Burke, Ibid; The attacks carried out by Anders Breivik on July 22, 2011, in Oslo and Utoya, in which 77 people lost their lives, were also an important breaking point

60 Timothy McVeigh is responsible for the 1995 Oklahoma City Alfred P. Murrah Federal Building bombing that killed 168 people, 19 of whom were children playing in the kindergarten of the building. The bombing was the deadliest attack in the US soil prior to the 9/11.

On the other hand, it can be seen that there is an illusion regarding the UNABOMBER. Kaczynski had his unique ideology, but in reality, every actor is somehow influenced by the information warfare tactics of terrorist organizations, and gives various low-level signals at the ideological level, even if not at the operational level. Although, as stated before, these signals are not easy to detect; this situation leads to comments that there is no such an attacker as a lone actor and this definition should be completely eliminated.[61]

4.2. Broad Conceptualization

Broad conceptualizations accept that none of the attackers is truly alone. Accordingly, the main question to be asked is not whether the lone actors are alone or not, but how alone he is.[62] Although broader definitions agree that it is very difficult for lone actors to be in an ideological vacuum, they differ on the operational linkage. While some studies reject the operational link and support,[63] others include it in the definition and argue that it is sufficient for the attacker to be alone at the time of action.[64] That is why this broadest definition encompasses all kinds of suicide attackers if they are alone at the moment of an attack. Broad conceptualization encompasses a large set of attacks and hybrid cases on a continuum.[65] According to Gill et. al. 20 of 119 (16.8%) lone-actor cases that they analyzed have a broader operational linkage.[66] In another work, 86% of lone actors give signals about their radicalization process and 58% of them give signals about their operational plans.[67]

---

61 For example, Bart Schuurman, Lasse Lindekilde, Stefan Malthaner, Francis O'Connor, Paul Gill, Noemie Bouhana, "End of the Lone Wolf: The Typology that Should Not Have Been", *Studies in Conflict & Terrorism*, 42(8) (2017), 771-778.

62 Feve, Bjornsgaard, Ibid, p.3

63 Gruenewald, et. al., Ibid, p.75; Bakker and Zuijdewijn, Ibid.

64 Feldman, Ibid, pp.281-282; Gill, et. al., Ibid, p.426; Barnea, Ibid, p.220; United Nations also use a broader definition and accepts that the individuals who go or attempt to go to conflict zones, develop radical discourse, and show interest in websites used by terrorist organizations are potential lone actor candidates. (United Nations, Ibid. (2015); This definition encompasses Foreign Terrorist Fighters (FTFs) that are defined as "individuals who travel to a State other than their State of residence or nationality for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict" according to "United Nations Security Council Resolution 2178", (2014), available at https://www.un.org/securitycouncil/s/res/2178-%282014%29 (accessed 03 October 2020);

65 Borum,et. al., Ibid, p.393

66 Gill, et. al., Ibid, p.430.

67 Schuurman, Ibid, p.774. For detailed information about signals and laekage behaviour see "Federal Bureau of Investigation Homegrown Violent Extremist Mobilization Indicators Booklet", (2019), available at https://www.dni.gov/files/NCTC/documents/news_documents/NCTC-FBI-DHS-HVE-Mobilization-Indicators-Booklet-2019.pdf, (accessed 20 October 2021)

There is a similar argument about dyads too. Dyads are some forms of a small cell configuration and that is why it can be thought that they should be excluded from the definition. On the other hand, these cells are either composed of family members or formed by the lone actor before the attack.[68] Cells made up of family members are especially resistant to infiltration. For example, dyads composed of relatives, such as married couples like San Bernandino attackers Rizwan Farook and Tashfeen Malik, or the Tsarnaev brothers who committed the 2013 Boston Marathon attack, have succeeded in secrecy.[69]

Another important issue about the ideological and operational linkage is the medium. The medium can be either physical or virtual. In particular, social media, which is defined as the "virtual community",[70] is a very important tool to disseminate discourse and give operational training. In this virtual community, potential attackers can access educational materials, meet other radicals and receive operational instructions. Some of them even establish a direct linkage with mentors like Anwar al-Awlaki and Rashid Rauf.

5. Analysis of the Attacks

In this part, the empirical findings of the al Qaeda- and Daesh-related attacks carried out in the European Union zone in 2009-2021 are analyzed. For this purpose, the attacks in the EUROPOL database have been examined under various subtitles.[71] There are a total of 89 al Qaeda- and Daesh-related attacks in the EUROPOL database. Out of a total of these 89 attacks, three of them were prevented while they were at the plotting stage[72] and there is no information found for one attack in open-source material.[73] These cases are excluded from the data set and 85 cases are examined.

---

68 Gill, et. al., Ibid, p.426.

69 Moreover, cells with a sophisticated organizational linkage also uses family dyads in their operations. Daesh members Şeyh Abdurrahman Alagöz and Yunus Emre Alagöz, who carried out suicide attacks in Ankara and Suruç in 2015, and the AQAP affiliated 2015 Charlie Hebdo attackers Cherif Kouachi and Saïd Kouachi were family dyads.

70 J. Reid Meloy, Jessica Yakeley, "The Violent True Believer as a 'Lone Wolf' Psychoanalytic Perspectives on Terrorism", *Behavioral Sciences and the Law*, 32(3) (2014), pp.347–365, p.353.

71 EUROPOL web site, Ibid.

72 According to the authorities, many plots with different degrees of organizational contact are prevented every year. On the other hand, since only three unsuccessful plots are included in the EUROPOL data, they are excluded from the study in terms of the reliability of the data set.

73 In Italy on 4 November 2019, a Liberian national launched a bottle rocket against a wall in Rome when he saw an army patrol. He was carrying in his backpack another bottle filled with petroleum. Although the action is reminiscent of other lone actor behavior, it was excluded from the research due to insufficient information in open sources.

In the literature, there are a few studies that used various subtitles for the analysis of the attacks carried out by these organizations. For example, in 2012, Borum et al. used this kind of classification under variables of *loneness, direction*, and *motivation*.[74] In 2019, Clemmow, et. al., used *propensity, situation*, and *network*.[75] In this study, classification is made by using ideological and operational connections. Attacks are codified in ideological linkage as: isolation, signaling-leakage behavior, on the radar, under surveillance, and physical connection. In operational linkage the codes are: isolation, online guidance, physical guidance, foreign terrorist fighter (FTF), and cell formation (Tables 1 and 2). EUROPOL dataset is classified under these dimensions (Table 3).

Table 1: Ideological Codificat

IDEOLOGICAL CONNECTION	
Isolation	0
Signaling – Leakage Behavior	1
On the Radar	2
Under Surveillance	3
Physical Connection	4

Table 2: Operational Codification

OPERATIONAL CONNECTION	
Isolation	0
Online Guidance	1
Physical Guidance	2
Foreign Terrorist Fighter	3
Cell Formation	4

[74] Borum et al. suggests that instead of debating definitions, it may be more useful to view each key feature along a continuum. See Borum, et. al., Ibid.

[75] Clemmow, et. al., Ibid.

		ATTACK	IDEOLOGICAL				OPERATIONAL			ORGANIZATIONAL SCORE	CRIME	MENTAL	TACTIC	IMMIGRANT	TARGET
			LEAKAGE	RADICAL	WATCH LIST	PHYSICAL	ONLINE	PHYSICAL	FTF	CELL						
1	2009 (12 October)	2009 Milano Santa Barbara Bombing - Mohammed Game	1							4	1-4			B	Y	M
2	2009 (25 December)	2009 Christmas Day Bombing Plot - Umar Farouk Abdulmutallab			3				3		3-3			B		C
3	2010 (1 January)	2010 Kurt Westergaard Attack - Mohamed Geele									0-0			ST	Y	C
4	2010 (27 June)	2010 Bugojno Bombing - Haris Causevic		2						4	2-4	Y		B		F
5	2010 (10 September)	2010 Hotel Jørgensen explosion - Lors Doukaiev									0-0			B	Y	C
6	2010 (11 December)	2010 Stockholm Bombing - Taimour Abdulwahab al-Abdaly	1					2			1-2			B	Y	C
7	2011 (2 March)	2011 Frankfurt Airport Shooting - Arid Uka									0-0			SH	Y	M
8	2012 (11-19 March)	2012 Toulouse and Montauban Shootings - Mohammed Merah		2				2			2-2	Y	Y	SH		M+C
9	2012 (October)	2012 Cannes-Torcy Cell Attacks								4	0-4			B		C
10	2013 (22 May)	2013 Woolwick Ramming - Michael Adebolajo and Michael Adebowale			3					4	3-4	Y		R+ST		M
11	2013 (25 May)	2013 La Defence Stabbing - Alexandre Dhaussy		2							2-0	Y	Y	ST		M
12	2014 (24 May)	2014 Brussels Jewish Museum Shooting - Mehdi Nemmouche		2					3		2-3	Y		SH		C
13	2014 (20 December)	2014 Tours Police Station Stabbing - Bertrand Nzohabonayo									0-0	Y		ST	Y	F
14	2014 (21 December)	2014 Dijon Ramming - Nacer B.									0-0	Y	Y	R		C
15	2014 (22 December)	2014 Nantes Ramming - Sébastien Sarron									0-0		Y	R		C
16	2015 (7 January)	2015 Charlie Hebdo Shooting - Said Kouachi and Chérif Kouachi				4				4	4-4	Y		SH		C
17	2015 (9 January)	2015 Kosher Market Shooting - Amedy Coulibaly			3					4	3-4	Y		SH		C

18	2015 (3 February)	2015 Nice Stabbing - Moussa Coulibaly			3					3 - 0	Y		ST			P
19	2015 (14 February)	2015 Copenhagen Shootings - Omar Abdel Hamid El-Hussein			3					3 - 0	Y		SH			C
20	2015 (26 June)	2015 Saint-Quentin Fallavier Attack - Yassin Salhi		2						2 - 0			ST			C
21	2015 (21 August)	2015 Thalys Train Attack - Ayoub El Khazzani			3			3		3 - 3			SH	Y		C
22	2015 (17 September)	2015 Berlin Police Stabbing - Rafik Yousef			3					3 - 0	Y		ST			P
23	2015 (13 November)	2015 Bataclan Attack				4			4	4 - 4			SH	Y		C
24	2015 (6 December)	2015 London Leytonstone Tube Station Stabbing - Muhaydin Mire								0 - 0		Y	ST	Y		C
25	2016 (7 January)	2016 Paris Police Station Attack Tarek Belgacem	1							1 - 0			ST	Y		P
26	2016 (11 January)	2016 Marseille Jewish Teacher Attack - 15 years of Boy								0 - 0			ST			C
27	2016 (26 February)	2016 Hanover Stabbing - Safia S.		2			2			2 - 2			ST			P
28	2016 (22 March)	2016 Brussels Airport and Metro Bombings				4			4	4 - 4			B			C
29	2016 (13 June)	2016 Magnanville Stabbing - Larossi Abballa		2						2 - 0	Y		ST			P
30	2016 (14 July)	2016 Nice Truck Ramming - Mohamed Lahouaiej-Bouhlel								0 - 0	Y		R			C
31	2016 (18 July)	2016 Würzburg Train Stabbing - Riaz Khan Ahmadzai					1			0 - 1			ST	Y		C
32	2016 (24 July)	2016 Ansbach Bombing - Mohammad Daleel						3		0 - 3		Y	B	Y		C
33	2016 (26 July)	2016 Saint-Étienne Church Stabbings - Adel Kermiche Abdel and Malik Petitjean			3					3 - 0		Y	ST			C
34	2016 (6 August)	2016 Stabbing of Charleroi Police Officers - Khaled Babbouri								0 - 0	Y		ST	Y		P
35	2016 (5 October)	2016 Stabbing of Brussels Police Officers - Hicham Diop		2						2 - 0			ST			C
36	2016 (19 December)	2016 Berlin Christmas Market Ramming - Anis Amri			3					3 - 0	Y		R	Y		C

39	2017 (20 April)	2017 Champs-Élysées Attack - Karim Cheurfi			3				3 - 0	Y	Y	SH		P
40	2017 (22 May)	2017 Manchester Arena Attack - Salman Ramadan Abedi	1				3		1 - 3	Y		B		C
41	2017 (3 June)	2017 London Bridge Attack - Khuram Shazad Butt Rachid Redouane Youssef Zaghba		2				4	2 - 4			R+ST	Y	C
42	2017 (6 June)	2017 Notre-Dame de Paris attack - Farid Ikken							0 - 0			H	Y	P
43	2017 (19 June)	2017 Champs-Élysées Ramming - Djaziri Adam Lotfi			3				3 - 0			R		M
44	2017 (20 June)	2017 Brussels Central Station Bombing - Oussama Zariouh							0 - 0	Y		B	Y	C
45	2017 (28 July)	2017 Hamburg Stabbing - Ahmad Alhaw			3				3 - 0			ST	Y	C
46	2017 (9 August)	2017 Paris Levallois-Perret Ramming - Hamou Benlatrèche							0 - 0	Y		R		M
47	2017 (17 August)	2017 Barcelona and Cambrils Attacks						4	0 - 4			R+ST+B		C
48	2017 (18 August)	2017 Turku attack - Abderrahman Bouanane							0 - 0			ST	Y	C
49	2017 (25 August)	2017 Buckingham Palace Sword Attack - Mohiussunnath Chowdhury							0 - 0			ST		P
50	2017 (25 August)	2017 Brussels Stabbing - Hasshi Ayaanle							0 - 0	Y	Y	ST	Y	M
51	2017 (15 September)	2017 Parsons Green Train Bombing - Ahmed Hassan			3		3		3 - 3			B	Y	C
52	2017 (1 October)	2017 Marseille Stabbing - Ahmed Hanachi							0 - 0	Y		ST	Y	C
53	2018 (5 May)	2018 The Hague Stabbing – Syrian National							0 - 0		Y	ST	Y	C
54	2018 (12 May)	2018 Paris Knife Attack - Khamzat Azimov			3				3 - 0			ST	Y	C
55	2018 (23 March)	2018 Carcassonne and Trèbes Attacks - Redouane Lakdim			3				3 - 0	y		SH	Y	C
56	2018 (29 May)	2018 Liège Attack - Benjamin Herman		2					2 - 0	Y		ST		P
57	2018 (31 August)	2018 Amsterdan Tourist Stabbing - Jawed Sultani							0 - 0			ST	Y	C

58	2018 (11 December)	2018 Strasbourg Shooting - Chérif Chekatt		3					3-0	Y		SH		C
59	2018 (31 December)	2018 Manchester Victoria Stabbing - Somalian National							0-0		Y	ST	Y	C
60	2019 (5 March)	2019 the Condé-sur-Sarthe Prison Stabbing - Michaël Chiolo		3					3-0	Y		ST		P
61	2019 (18 March)	2019 Utrecht Tram Shooting - Gökmen Tanış							0-0	Y	Y	SH		C
62	2019 (24 May)	2019 Lyon Parcel Bombing - Mohamed Hichem Medjoub							0-0			B	Y	C
63	2019 (17 September)	2019 Milano Stabbing - Mahamad Fathe							0-0		Y	ST	Y	M
64	2019 (3 October)	2019 Paris Police Headquarters Stabbing - Mickaël Harpon	1						1-0		Y	ST		P
65	2019 (29 November)	2019 London Bridge Stabbing - Usman Khan		3					3-0			ST		C
66	2020 (3 January)	2020 Paris Villejuif Stabbings - Nathan C							0-0		Y	ST		C
67	2020 (9 January)	Whitemoor Prison Stabbing - Brusthom Ziamani		3				4	3-4			ST		P
68	2020 (2 February)	Streatham Stabbing - Sudesh Amman		3	1				3-1			ST		C
69	2020 (4 April)	2020 Romans-sur-Isère Stabbing - Abdallah Ahmed-Osman							0-0			ST	Y	C
70	2020 (27 April)	2020 Paris Colombes (Hauts-de-Seine) Ramming - Youssef T.							0-0			R		P
71	2020 (April - May)	2020 Waldkraiburg Arson Attacks - Muharrem D.	1						1-0			A		C
72	2020 (20 June)	Reading Stabbings - Khairi Saadallah			4		3		4-3	Y		ST	Y	C
73	2020 (18 August)	2020 Berlin Highway Ramming - Samrad A.							0-0			R	Y	C
74	2020 (12 September)	2020 Morges Stabbing		3					3-0			ST		C
75	2020 (25 September)	2020 Paris (Charlie Hebdo) Stabbing							0-0			ST	Y	C

76	2020 (16 October)	2020 Murder of Samuel Paty - Abdoullakh Abouyezidovich Anzorov	1	1		1-1	ST	Y	C
77	2020 (29 October)	2020 Nice Notre Dame Stabbing - Brahim Aoussaoui				0-0	ST	Y	C
78	2020 (4 October)	2020 Dresden Stabbing - Abdullah al-H		3	1	3-1	ST	Y	C
79	2020 (2 November)	2020 Vienna Shooting – Kujtim Fejzulai		3		3-0	SH		C
80	2020 (24 November)	2020 Lugano Stabbing		2		2-0	ST		C
81	2021 (23 April)	Rambouillet Stabbing - Jamel Gorchene				0-0	ST	Y	P
82	2021 (17 September)	Murcia Ramming - Abdellah Gmara				0-0	ST	Y	C
83	2021 (15 October)	Murder of David Amess - Ali Harbi Ali		2		2-0	ST		C
84	2021 (6 November)	Bavaria Train Stabbing - Syrian national				0-0	ST	Y	C
85	2021 (14 November)	Liverpool Hospital Bombing - Emad al-Sweailmeen				0-0	Y	B	Y	C

Table 3: Classification of Attacks in European Union Zone Between 2009-2021[76]

[76] Table is prepared by the authour.

A: Arson

B: Bombing

C: Civilian[77]

P: Police Officer

M: Military Personnel

R: Ramming

SH: Shooting

ST: Stabbing

Y: Yes

According to the empirical results, 33 of the total 85 attacks (39%)[78] did not have an organizational link, either operationally and ideologically. These cases fit into the narrow definition of lone-actor attacks. These attackers either did not give any signals before the attack or low-intensity signals were not detected by the security forces. It is obvious that lone actors are radicalized ideologically, on the other hand, this process developed passively and very rapidly. As it will be stated later, the processes were developed in an unpredictable and fuzzy way and in some instances due to the effects of mental disease. Due to their unique characteristics, in this study these cases are accepted as lone-actor attacks.

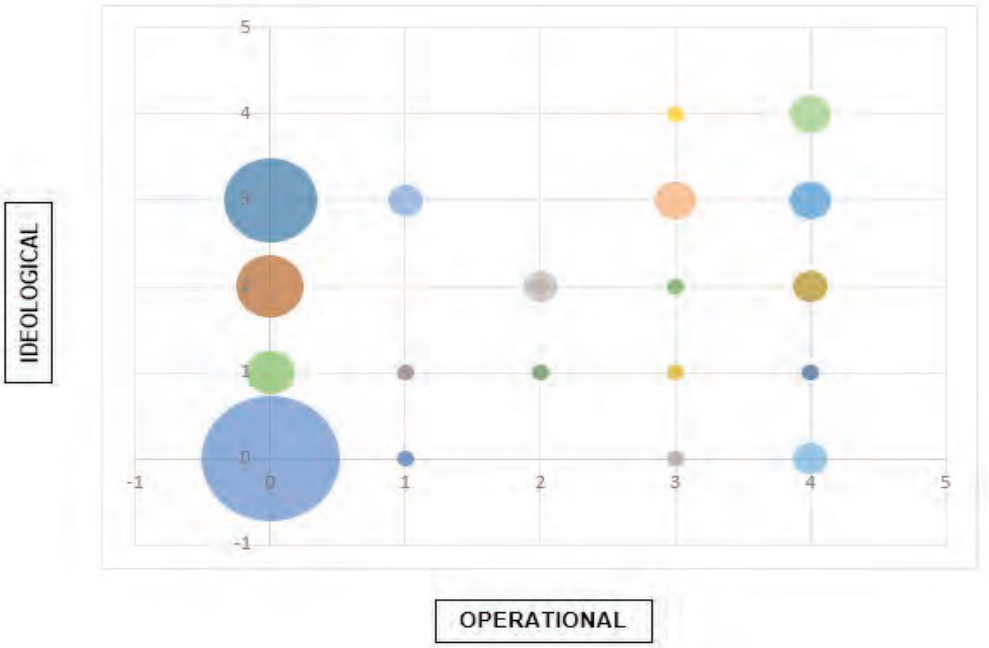
Table 4: Classification of al Qaeda and Daesh Affiliated Attacks

		OPERATIONAL				
		0	1	2	3	4
IDEOLOGICAL	0	33	1		1	2
	1	4	1	1	1	1
	2	8		2	1	2
	3	15	2		3	3
	4				1	3

[77] British MP Davis Amess is counted as a civilian

[78] Marked grey in the table

Graph 1: Classification of al Qaeda and Daesh Affiliated Attacks



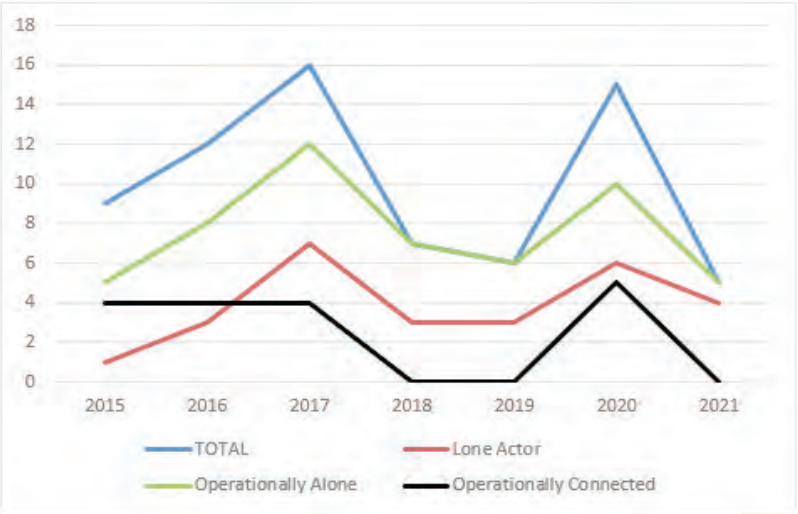
According to the empirical data, since 2015, the most intense threat has been coming from operationally isolated attackers (Graph-2). Of course, this does not mean that FTFs and cells are not a threat anymore. This result can be a survivor bias and can also be interpreted as the result of successful counter-terrorism efforts of security agencies in the prevention of operational cells.[79] It is known that many plots have been prevented, not only in the European Union zone, but also in countries like Türkiye and the USA. On the other hand, there is no accurate comprehensive database of plots stopped during the preparation phase. It can be interpreted that the reasons for the decrease in the number of attacks with operational connections after 2017[80] are decreased capacity of al Qaeda and Daesh, the slowdown of the migration wave, and the increase in the capacity and cooperation of counter-terrorism intelligence.

---

79 Some of these cells are directly connected with combat zones like the Bataclan attackers. On the other hand, most of them are formed as radical milieus and not connected to the core structures. For description of radical milieu see Stefan Malthaner, Peter Waldmann, "The Radical Milieu_ Conceptualizing the Supportive Social Environment of Terrorist Groups", *Studies in Conflict & Terrorism*, 37(12) (2014) pp.979-998

80 As it can be seen there is a dramatic increase in operationally connected attacks in 2020. On the other hand, three out of five attackers are just operationally directed online (Operational Connection Scale - 1) and two of them were under surveillance.

Graph 2: Distribution of Attacks Between 2015-2021



Lone actors in Europe have diverse backgrounds. For example, Farid Ikken, who carried out a knife attack against police officers on duty in Notre-Dame de Paris in 2017, was a journalist who came to France for doctoral education; in 2009 he was awarded the National Journalist Prize from the European Commission for his reports on human rights. He grew up in a secular environment and did not show any signs of radicalization before the attack. On the other hand, a video of Ikken was found during a search of his house, swearing allegiance to Daesh.[81]

Another attacker who was classified as a lone actor is Moroccan national Hamou Benlatrèche. He rammed his car into a group of soldiers near Paris on August 9 of 2017. According to the statement of the prosecutor's office, no connection of the attacker with Daesh was detected. On the other hand, it was also stated that after the technical analysis of Benlatrèche's cellphone and computer, it was found that he followed Daesh-related forums and conducted research on crossing into Syria.[82]

---

81 "Notre Dame Attacker 'Pledged Allegiance to IS in Video'", (07 June 2017), *France24*, available at https://web.archive.org/web/20170719031955/http://www.france24.com/en/20170607-notre-dame-attacker-pledged-allegiance-video, (accessed 20 March 2021).

82 "Man Arrested in French Car Attack had Radical Beliefs", *The Washington Times*, (23 August 2017), available at https://www.washingtontimes.com/news/2017/aug/23/man-arrested-in-french-car-attack-had-radical-beli/ (accessed 20 March 2021).

Similarly, 2011 Frankfurt Airport shooter Arid Uka never had physical contact with an extremist network. His sole organizational contact was online and he radicalized himself by watching propaganda videos.[83] This is the common story of many lone actors. They were radicalized ideologically, but unlike attackers like Nidal Hassan,[84] they did not engage in any kind of an organizational connection, except for passive research.

If we use a broader conceptualization of the lone-actor definition and include those who gave strong signals of ideological radicalization, this number rises to 60 (70.5%). This rate rises to 76% between 2015 and 2021, when the frequency of attacks dramatically increased in the European Union zone. On the other hand, it is impossible to pinpoint the attacker because there are thousands of individuals showing similar signals. As in the French case, mass internment does not yield any results either. This is the most important dilemma created by lone actors.

The degree of ideological linkage involved in broad conceptualization varies case by case. Mickaël Harpon is an example of signaling (Rate 1-0). Harpon was an IT specialist in the intelligence unit of the Paris police headquarters when he stabbed four of his colleagues to death on 3 October 2019. There were signals of his radicalization, but these signals were not taken seriously. He had changed his life style dramatically; in 2015, some of Harpon's colleagues reported his praise for the Charlie Hebdo attack.[85]

In some cases, radicals enter the radar of the police forces but engage in an attack anyway (Rate 2-0). For example, Hicham Diop, who attacked the police officers on duty in Brussels Schaerbeek on 5 October 2016 with a machete, can be included in this classification. Diop, who was an army veteran and a candidate for a chair in the local parliament, was known to Belgian authorities due to his links with radicals who traveled to Syria.[86]

---

83 "Frankfurt Airport Shooting may have Islamist Link, Say Police", *The Guardian*, (03 March 2011), available at https://www.theguardian.com/world/2011/mar/03/frankfurt-airport-shooting-islamist-link? (accessed 25 March 2021)

84 Major Nidal Hassan who was a psychiatrist in the US Army, killed 12 people at the Fort Hood military base on October 5, 2009. Although Hassan has not physically connected to the conflict zones, he has received online ideological and operational mentorship from the AQAP cleric al Awlaki. As it was committed in USA, this case was not included in this research.

85 "Paris Police Killings: Minister Calls for 'Automatic Alerts'", *BBC*, (07 October 2019), available at https://www.bbc.com/news/world-europe-49959827 (accessed 25 March 2021).

86 "Brussels Police Stabbed in 'Terror Attack'", *BBC*, (5 October 2016), available at https://www.bbc.com/news/world-europe-37563836 (accessed 25 March 2021).

The next level of ideological connection for broad definition is attacks committed by actors who are under surveillance (Rate 3-0). These attackers were known to security forces; they were under physical or technical surveillance. Anis Amri, who killed 13 people and injured 55 people in the Christmas market truck attack in Berlin on 19 December 2016, is an example of lone actors who were on the watch list of the security agencies. Three weeks before the attack, a note from Moroccan intelligence stated that Amri was in search of a terrorist attack, but he could not be deported because the legal process had not been finalized and he had not made an operational contact.[87]

There is no attacker that fits into the highest level of ideological connection (Rate 4 – 0). It seems coherent because radicals that had established physical connection with overseas prior to the attack were generally FTFs. In our dataset they are FTFs like Bataclan and Charlie Hebdo attackers.

After this initial analysis, the common attributes of lone actors are examined. According to the empirical data, actors without organizational linkage still pose a real threat to the European Union. These actors differ from other attackers not only in organizational connection but also in other variables like mental health, lone actor-crime nexus, legal status, target selection, and tactics (Table-5).

Table 5: Comparison of Different Type of Attacks (Numbers are percentage)[88]

	Overall Ratio	Crime	Mental	Immigrant	Target (Civilian)	Tactics (Stab+Ram)
Lone Actor	39	30	27,5	73	69,5	81,5
Operationally Alone	70,5	36,5	21,5	50	66,5	80
Operationally Connected	29,5	32	8	44	76	36
Total	100	35	17.5	48	69,5	60

87 "Berlin Islamist Terror Attack: A Deadly Story of Failure", *Deutsche Welle*, (18 December 2020), available at https://www.dw.com/en/berlin-islamist-terror-attack-a-deadly-story-of-failure/a-55990942 (accessed 25 March 2021).

88 Table is prepared by the author according to the empirical findings.

5.1. Mental Health

As lone actors do not have strong organizational or social linkage, psychological factors are at the center of this radicalization process. In this sense, there is a meaningful relationship between lone actor attacks and mental illness. 9 out of 33 (27.5%) of the actors have mental issues. The ratio for attackers with operational linkage is only 8%. Although these ratios are based on open-source analysis and are thus disputable, the margin is dramatic.

It can be seen that the ratio of mental illness is slightly higher than the population average.[89] On the other hand, this does not weaken the ideological dimension of the attack. It is accepted that the paranoid fantasies of violent individuals with mental illness are manipulated by al Qaeda and Daesh. Actors with mental issues are manipulated by online propaganda; as the visibility of these organizations in the media increases, it becomes easier to manipulate people with mental illnesses.[90] At this point, the pull effect of information warfare becomes visible. These actors may have biological, psychological, or sociological motives, but they reflect their reactions through terrorist organizations.

This result inevitably causes contradictory arguments about attacker motivation. For example, one of these attackers, Sébastien Sarron, who had mental problems and committed suicide in prison in 2016, confused the minds of the French politicians. French Interior Ministry spokesman Pierre-Henry Brandet officially declared in the immediate wake of the attack that *"I wouldn't say it was a terrorist attack. I would call it a deliberate act"*.[91] On the other hand, according to the EUROPOL, this attack had been motivated by Daesh's online propaganda and was thus classified as a terrorist attack.[92]

5.2. Lone Actor-Crime Nexus

The pull factor of information warfare is also effective on lone actor-crime nexus. A significant number of lone actors are converts, drug addicts, and petty criminals who have a record of violent behavior. Just as with mental illness, 10 out of 33 (30%) lone actors have a criminal background. For example, the Nice

---

89 According to a study this rate is around 25% in the general population. Jordi Alonso et al., "Prevalence of Mental Disorders in Europe: Results from the European Study of the Epidemiology of Mental Disorders (ESEMeD) Project," *Acta Psychiatrica Scandinavica,* (109) (2004), pp.21–27, p.24

90 "Global Terrorist Groups Exploit Mentally ill People to Carry Out Attacks: Experts", *The Straits Times,* (12 May 2016), available at https://www.straitstimes.com/world/global-terrorist-groups-exploit-mentally-ill-people-to-carry-out-attacks-experts (accessed 25 March 2021).

91 **"**France to Deploy Soldiers after Spate of Attacks, *BBC*, (23 December 2014), available at https://www.bbc.com/news/world-europe-30586798 (accessed 25 March 2021).

92 "European Union Terrorism Situation and Trend report 2015", (European Police Office 2015), p.19.

attacker Mohamed Lahouaiej-Bouhlel, who came to France from Tunisia in 2005, had a record of drug addiction and crimes such as domestic violence and sexual assault during his years in France. He did not show signs of radicalization in the organizational sense until a short time before his attack.

Criminality is also relevant for FTFs and other cell formations. That is why Alain Grignard, the head of Brussels Federal Police describes Daesh as a *"sort of a super-gang"*.[93] In this manner, redemption and life embeddedness[94] are important motives of action. Radical ideology seems to be an important means of salvation for those who want to be purified from their criminal past. In particular, organizations such as Daesh that do not demand religious knowledge and background for membership are seen as an important pull factor in this process.[95] Individuals are pushed to radicalism by criminal background and pulled by radical narratives of Deash. In Daesh's narrative, this is formulated as *"sometimes people with the worst pasts create the best futures"*.[96]

5.3. Legal Status

One of the important attributes of lone actors is that they are homegrowns or immigrants rather than homecomings or FTFs. In general, 48% of the attackers are immigrants. This number increases to 73% (24 out of 33) in lone-actor cases. Some people argue that these immigrants are FTFs and they are intentionally sent to Europe with a cover story to commit an attack. For example, some members of the terrorist cell that carried out the 2015 Bataclan attack were foreign nationals who came to France with an asylum-seeker cover.[97] In these kinds of scenarios, attackers quickly turn to their task and act as cells. On the other hand, in lone-actor cases, the attackers do not directly engage in an attack immediately. Most of them try to assimilate into their new country. For example, the 2020 Romans-sur-

---

93 Paul Cruickshank, "A View from the CT Foxhole: An Interview with Alain Grignard, Brussels Federal Police", *CTC Sentinel*, 8(8) (2015), pp.7-10, p.8.

94 "*All people aspire to create a solidly embedded life and that perceived life embeddedness…good life embeddedness can be defined as a good match between life tasks and life competencies. Threatened life embeddedness can thus be defined as a mismatch…people who experience threats to their life embeddedness will strive to (re)establish embeddedness…in rare cases, the search to (re) establish life embeddedness and reduce uncertainty can lead to political or religious radicalization.*" Lasse Lindekilde, Preben Bertelsen and Michael Stohl. "Who Goes, Why, and With What Effects: The Problem of Foreign Fighters from Europe", *Small Wars and Insurgencies*, 27(5) (2016), pp.858-877.

95 Basra, et. al., Ibid, p.24.

96 A propaganda poster of British radical group Rayat al-Tawheed cited in Basra, et. al., Ibid, p.7.

97 "Paris attacks: Who were the attackers?", *BBC*, (27 April 2016), available at https://www.bbc.com/news/world-europe-34832512 (accessed 16 October 2021); In the literature these kinds of attackers are called the "sixth column".

Isère attacker, Abdallah Ahmed-Osman, was a Sudanese immigrant who received asylum status in 2017. During the search of his home, handwritten documents were found in which the author of the lines complained, in particular, of living in a land of disbelievers.[98] Another example is the 2015 London Leytonstone Tube Station attacker Muhaydin Mire, who came to the UK as a child. That is why the lone actor-immigration nexus seems like a psychological and sociological issue rather than a tactical cover.[99]

As we move towards the right side of the graph, the profile of the attacks dramatically changes. These attacks are usually carried out by the homecomings or cell structures that used more sophisticated techniques and tactics. Emni had a vital role in these attacks. It is considered that the 2015 Paris/Brussels, May 2014 Jewish Museum Brussels and August 2015 Thalys train shooting, the 2016 Berlin Christmas Market attack, and the 2017 Manchester concert attack were organized and executed by Emni elements in Libya.[100] Al Qaeda also executed terror attacks in this era. Saïd Kouachi, who was one of the Charlie Hebdo attackers, had been to Yemen in 2011, met al Awlaki, and trained in AQAP camps.[101]

5.4. Targets

Although lone actors prefer civilians as targets, the ratio is significantly lower than the operationally connected attackers. 69.5% (23 out of 33) of the victims are random civilians, others are hard targets like police officers and soldiers. They generally target symbolical places like museums and dates like Bastille Day. On the other hand, as they don't make organizational contact, it is hard to detect them in a target-centric approach. Even the terrorist organization will not know the timing of an attack. One of the challenges for authorities is the difficulty of tracking every person with bad intentions before they get out of control. That is why maybe the best way of deterring lone actors and protecting critical assets is denying the area by a preponderance of effort. In this effort, military personnel also have an important role. During Operation Sentinelle about 10000 soldiers and 4,700 police and gendarmes

---

98 "Attaque de Romans-sur-Isère : Les Premiers Éléments de l'enquête", *L'Obs*, (04 April 2020), available at https://www.nouvelobs.com/terrorisme/20200404.OBS27072/romans-sur-isere-les-premiers-elements-de-l-enquete.html (In French) (accessed 08 October 2021)

99 "Leytonstone knife attack: man convicted of attempted murder", *The Guardian*, (08 June 2016), available at https://www.theguardian.com/uk-news/2016/jun/08/leytonstone-knife-attack-man-convicted-of-attempted (accessed 16 October 2021).

100 Sutherland, ibid; Clarke, ibid.

101 "Both brothers behind Paris attack had weapons training in Yemen: sources", *Reuters*, (11 January 2015), available at https://www.reuters.com/article/us-france-shooting-yemen-idUSKBN0K-K0F620150111 (accessed 08 October 2020)

were deployed in critical places of France.[102] Similarly, in Belgium, Italy, and the United Kingdom, thousands of military personnel deployed in the cities to deter and deny the area for terrorist attacks. On the other hand, even if the military is used to reach a preponderance, it is impossible to control all areas. As Bavarian Interior Minister Joachim Herrman declared after the Würzburg Train stabbing, *"Police needed to be strengthened but it was clear that authorities could never guarantee 100 percent safety for citizens. There cannot be a police officer in every train. A lone attacker with a knife or axe could theoretically strike anywhere in Germany."*[103]

An important result of this deployment is the increase in counterforce attacks. Especially in France, police officers and military personnel serving within the framework of Operation Sentinelle were frequently targeted. Between 12 January 2015, the date that Operation Sentinelle began, and 23 April 2021, 11 out of 27 attacks (40.5%) carried out in France targeted police and soldiers. It is not known whether the increase in the visibility of the soldiers acts as a catalyst for the radicals. On the other hand, obviously, uniformed personnel attract attackers like a magnet. Maybe, just as in sting operations, uniformed personnel facilitate and accelerate the transition process of a radical and save civilian lives. In this respect Colonel Pierre-Olivier Marchand states, *"Our soldiers do not see themselves as targets but as shields…it is better that (the actors) attack soldiers who are able to react in the appropriate manner…it is difficult to say if and how many attacks have been avoided thanks to this operation, but I am convinced it has an effect against the 'opportunity terrorists'."*[104]

5.5. Tactics

Lone actors are single attackers with simple weapons. This is a direct result of the absence of operational contact. The signature tactics of lone actors are stabbing and ramming. 21 (63.5%) of lone actor attacks were stabbing[105] and 6 (18%) of them were ramming. This means that 81.5% of the attacks are improvised. This is also valid for the broad conceptualization. 48 out of 60 (80%) of the operationally isolated actors used stabbing or ramming as a tactic.

---

[102] "French police search home of man suspected of driving into soldiers", *The Guardian*, (09 August 2017), available at https://www.theguardian.com/world/2017/aug/09/paris-police-hunt-driver-hit-soldiers-on-patrol-levallois-perret (accessed 08 October 2020)

[103] "Several injured in attack on train near Würzburg, southern Germany", *Deutsche Welle*, (18 July 2016), https://www.dw.com/en/several-injured-in-attack-on-train-near-w%C3%BCrzburg-southern-germany/a-19408848 (accessed 08 October 2021)

[104] Interview with Commander of Task Force East Colonel Pierre-Olivier Marchand in Phillip Andrews, "News from The Front Operation Sentinel French Homeland Security Operation: Insights from Colonel Pierre-Olivier Marchand", (Center for Army Lessons Learned (CALL) 2018)

[105] One attack is conducted by a hammer.

There are three important points about these improvised attacks. Firstly, although these attacks are simple, they can have serious consequences. The most striking of these attacks was the 2016 Nice truck ramming. Lahouaiej-Bouhlel, who did not show notable ideological or operational signals, killed 86 people as a result of the attack he carried out in July 2016. Secondly, these attacks resemble suicide attacks. Although they do not directly kill themselves like suicide bombers, their attacks are some kind of a high-risk suicide mission. At the end of the attack, they are either killed or fatally wounded by police forces or military personnel. That is why in the literature, these kinds of attacks are called "*suicide by cop"*.[106] Another point related to the tactics has to do with the financing of attacks. Since the actions are carried out with very low budgets, there is no money traffic to be followed. It is enough to go to a shopping mall and buy a knife or rent a car just before the attack. Executing attacks with simple weapons reduces the signals before the attack. These attackers, who do not download explosive formulas from the internet or try to obtain flammable materials or firearms, do not leave traces to be followed.

On the other hand, the characteristics of attacks dramatically change as the operational linkage emerges. Only 36% (9 out of the 25) of operationally connected attacks are committed by simple tactics. If we exclude online recruited attackers, this ratio drops to 20%. The other 80% of attacks are mass shootings or bombings like the 2015 Bataclan and 2015 Thalys train attacks.

6. Conclusion

In this article, the concept of lone actor, which has gained popularity again recently, was discussed within the framework of organizational connection. For this purpose, first of all, the definition of lone actor is conceptualized. The definition of lone actor used in the study is attackers who do not establish an organizational contact at the ideological and operational level. As the organizational connection increases, the lone-actor characteristics decrease.

It is argued that al Qaeda- and Daesh-inspired lone actors are real and they constitute a significant threat to global security. Lone-actor attacks are executed in isolation and that is why they can be classified separately from other attackers like FTFs and cell formations. To operationalize this hypothesis, the data of EUROPOL's Annual European Union Terrorism Situation and Trend Reports are used. According to the empirical research, only 29.5% of the attacks in the European Union zone

[106] For detailed information see Christina Patton, William Fremouw. "Examining 'Suicide by Cop': A Critical Review of the Literature, *Aggression and Violent Behavior* (27) (2016) pp.107–120.

between 2009 and 2021 were operationally connected with al Qaeda or Daesh. 70.5% of the perpetrators were operationally isolated and 39% of them were both operationally and ideologically isolated.

Lone actors have signature attributes. First of all, their attacks are improvised and simple. 81.5% of lone-actor attacks are stabbing and ramming, while FTFs and cells use sophisticated tactics like mass shootings and bombings. Only 20% of operationally connected attacks are stabbing and ramming. Secondly, mental illness is significant in lone-actor behavior. 27.5% of them have mental issues which are significantly higher than the operationally connected attackers. Thirdly, although their main targets are civilians, lone actors also frequently select hard targets. 30.5% of their targets are soldiers and police officers. This ratio is 24% in operationally connected attackers. On the other hand, it is not known whether the uniform pulls attackers and triggers lone-actor behavior or not. Lastly, immigrants are an important pool for lone-actor attacks. According to statistical results, 73% of lone actors are immigrants.

In 2022, the center of gravity of Daesh attacks shifted to Afghanistan and Africa. Especially after the Taliban seized power in Afghanistan, several bombings were carried out in Kabul due to the power struggle between the new government and Daesh. There has also been a large increase in lone-actor attacks in Israel. From 22 March to 5 May, five terrorist attacks were committed in Israel. On the other hand, there has been a dramatic decrease in attacks in Europe. It can be considered that this is a capacity problem for the organizations rather than a conscious choice. It is known that after the killing of Daesh leader Abu Ibrahim al-Qurayshi, the organization called for stabbing and ramming attacks against Europe and the USA. In addition, it can be evaluated that al Qaeda will seek attacks in retaliation for the killing of its leader Ayman al-Zawahiri. EUROPOL's report for 2022 will give a clearer view of the security status of the European Union.

After conceptualizing the threat, in this part, the author would also like to quickly emphasize some tactical dimensions of countering these attackers. Since these types of attackers are not a part of a cell or do not have a physical or cyber connection with a larger network, it is very hard to detect them by intelligence means. Maybe the only way of preventing them is to deny both the physical and cyber terrain.

Firstly, physical area denial is the best option when security forces cannot simply rely on intelligence due to the severity and characteristics of a specific terrorist threat. But physical area denial needs preponderance and it is out of the limits

of the law enforcement agencies. That is why it is a collective effort of all security community. When necessary, military units should also be used for covering an area, protecting the potential targets, and deterring potential attackers. Accordingly, military units located in the urban landscape should be trained for counter-terrorism missions and their code of conduct should be clearly defined. It can be said that the military area-denial task is a new normal for countering terrorism.

Secondly, just like denying a physical terrain, security agencies should deny the cyber terrain. Although Foreign Terrorist Fighters like Reina attacker Masharipov or Paris attacker Abdelhamid Abaaoud were not active on the cyber terrain, most of the radicals and lone attackers are traceable on the web. Radical websites and social media platforms offer not only ideological indoctrination but also practical online training courses that urge visitors to take action on their own. Accordingly, outreach by security agencies into these online radical communities is key to providing early threat warnings. After filtering potential attackers, intelligence agencies can take other preventive measures. These measures are generally enhanced by clandestine physical and technical surveillance. In this context, sting operations can also be utilized. Cyber denial should also involve a close relationship between security agencies and commercial companies. Security agencies cannot cope with that huge amount of unstructured global data. Internet companies can assist security forces in identifying red flags and signals. In this manner, internet companies such as Google and Meta are on the front line of combatting radicalization and terrorism.

In conclusion, although some researchers argue that the definition of lone actor should be removed from the literature, the empirical results show that lone actors are a real threat to the European Union. In particular, attackers who do not connect operationally (those concentrated on the left vertical axis of the Graph-1) differ dramatically from those who have connections at the operational level (those on the right side of the Graph-1). Lone actors radicalize from a distance and do not physically connect with the organization. Rather than operate as part of a sleeper cell, they are normal people who go about their normal lives up to a point despite intense psychological pressure. Their actions are unsophisticated, and even after the action is taken, it cannot be understood for a long time whether it is a terrorist act. This organizational isolation is the main driving factor of a lone actor-based strategy for terrorist organizations. Since the late 19th century, it has been used by terrorist organizations with different ideologies. As a proven unconventional method, in the future, lone-actor attacks will most likely continue to be an important choice for terrorist organizations.

Bibliography

"A Former MI5 Agent Tells us Why it's so Easy for Terror Suspects like Khalid Masood to Move Around without Being Arrested", *Business Insider*, available at http://uk.businessinsider.com/mi5-agent-surveillance-of-islamic-terrorist-suspects-2017-3 (Accessed in 12 November 2020).

Al-Adnani Abu Muhammad, "Indeed Your Lord Is Ever Watchful", (9 September 2014)

Alami Mona, "Parsing the Islamic State's Nice Attack Claims" (19 July 2016) available at http://www.atlanticcouncil.org/blogs/menasource/parsing-the-islamic-state-s-nice-attack-claims, (accessed 11 May 2020)

Alonso, Jordi et al., "Prevalence of Mental Disorders in Europe: Results from the European Study of the Epidemiology of Mental Disorders (ESEMeD) Project," *Acta Psychiatrica Scandinavica,* (109) (2004), pp.21–27

"Al-Qaeda Chief Zawahiri Urges 'Lone-Wolf' Attacks on U.S.", *BBC*, (13 September 2013, https://www.bbc.com/news/world-middle-east-24083314 (accessed 20 October 2021)

Andrews Phillip, "News from The Front Operation Sentinel French Homeland Security Operation: Insights from Colonel Pierre-Olivier Marchand", (Center for Army Lessons Learned (CALL) 2018)

"Attaque de Romans-sur-Isère: Les Premiers Éléments de l'enquête", *L'Obs*, (04 April 2020), available at https://www.nouvelobs.com/terrorisme/20200404.OBS27072/romans-sur-isere-les-premiers-elements-de-l-enquete.html (In French) (accessed 08 October 2021)

Bakker Edwin, de Graaf Beatrice, "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed", Perspectives on Terrorism, 5(5-6) (2011), pp.43-50.

Bakker Edwin, Zuijdewijn Jeanine de Roy van, "Countering Lone-Actor Terrorism Series No. 2", (Royal United Services Institute for Defence and Security Studies Lone-Actor Terrorism Definitional Workshop 2015)

Barnea Avner, "Challenging the 'Lone Wolf' Phenomenon in an Era of Information Overload", *International Journal of Intelligence and Counterintelligence*, 31(2) (2018), pp.217-234.

Barnes Beau, "Confronting the one-man Wolf Pack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism", *Boston University Law Review*, (92) (2012), pp.1613-1662.

Basra Rajan, Neumann Peter and Brunner Claudia, "Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus, The International Centre for the Study of Radicalisation and Political Violence (ICSR) 2016)

Bates Rodger, "Dancing with Wolves: Today's Lone Wolf Terrorists", *The Journal of Public and Professional Sociology*, 4(1) (2012), pp.1-14.

Beam Louis, "Leaderless Resistance", *The Seditionist*, (12 February 1992), available at http://www.louisbeam.com/leaderless.htm. (Accessed 10 May 2020).

Bergen Peter "David Petraeus: ISIS is on its Way to Defeat but Terrorism Threat Persists", CNN, available at https://edition.cnn.com/2016/06/22/opinions/bergen-interview-with-petraeus/index.htm, (Accessed 20 October 2021)

Berger J.M., "The Boy Who Cried Lone Wolf", (12 February 2012), Foreign Policy, available at https://foreignpolicy.com/2012/02/21/the-boy-who-cried-lone-wolf/. (accessed 10 June 2020)

"Berlin Islamist Terror Attack: A Deadly Story of Failure", *Deutsche Welle*, (18 December 2020), available at https://www.dw.com/en/berlin-islamist-terror-attack-a-deadly-story-of-failure/a-55990942 (accessed 25 March 2021)

Borum Randy, "Loner Attacks and Domestic Extremism Informing Lone-Offender Investigations", *Criminology & Public Policy*, 12(1) (2013), pp.103-112.

Borum Randy, Fein Robert and Vossekuil Bryan, "A Dimensional Approach to Analyzing Lone Offender Terrorism", *Aggression and Violent Behavior*, 17(5) (2012), pp.389–396.

"Both brothers behind Paris attack had weapons training in Yemen: sources", *Reuters*, (11 January 2015), available at https://www.reuters.com/article/us-france-shooting-yemen-idUSKBN0KK0F620150111 (accessed 08 October 2020)

Briggs Rachel, "The Changing Face of al Qaeda", (Institute for Strategic Dialogue January 2012)

"Bringing Terrorists to Justice: Challenges in the Prosecution of Terrorists Acting Alone or in Small Cells", (United Nations 2015). https://www.un.org/sc/ctc/wp-content/uploads/2015/09/S_2015_123_EN.pdf.% (accessed 03 October 2020)

"Brussels Police Stabbed in 'Terror Attack'", BBC, (5 October 2016), available at https://www.bbc.com/news/world-europe-37563836 (accessed 25 March 2021)

Burke Jason, "The Myth of the 'Lone Wolf' Terrorist", The Guardian, (30 March 2017), https://www.theguardian.com/news/2017/mar/30/myth-lone-wolf-terrorist#img-4 (Accessed 03 March 2021)

Burton Fred, Stewart Scott, "The 'Lone Wolf' Disconnect", (30 January 2008), The Stratfor, available at www.stratfor.com/weekly/lone_wolf_disconnect, (accessed 10 May 2020).

Chmaytelli Maher and Kalin Stephen and Abdelaty Ali "Islamic State Calls for Attacks on the West during Ramadan in Audio Message", Reuters, available at https://www.reuters.com/article/us-mideast-crisis-islamicstate-idUSKCN0YC0OG, (accessed 15 June 2021).

"CIA Chief: Al Qaeda Poised to Attack U.S.", *CBS* (2010). https://www.cbsnews.com/news/cia-chief-al-qaeda-poised-to-attack-us/. (accessed 05 June 2020).

Clarke Colin, "Predicting the Next ISIS", (08 October (2018), available at https://nationalinterest.org/feature/predicting-next-isis-32822 (accessed 24 May 2020)

Clemmow Caitlin, Bouhana Noémie, and Gill Paul, "Analyzing Person-Exposure Patterns in Lone-Actor Terrorism", *Criminology & Public Policy*, 19(2) (2019), pp.1-31.

Cohen Gili, “Eizencott: Out of 101 Knives Attacks We Did Not Have Even One Warning,” Haaretz (18 January 2016), http://www.haaretz.co.il/news/ politics/1.2824704 (Hebrew)

Colquhoun Cameron, “Tip of the Spear? Meet ISIS’ Special Operations Unit, Katibat al-Battar”, (16 February 2016), *Bellingcat*, available at https://www.bellingcat.com/news/mena/2016/02/16/tip-of-the-spear-meet-isis-special-operations-unit-katibat-al-battar, (accessed 15 June 2021).

Corner Emily, Gill Paul, and Mason Oliver, “Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence” *Studies in Conflict & Terrorism* 39(6) (2016), pp.560-568.

Cruickshank Paul, “A View from the CT Foxhole: An Interview with Alain Grignard, Brussels Federal Police”, *CTC Sentinel*, 8(8) (2015), pp.7-10.

de Bourmont Martin, M., “Rights Advocates Brace for Anti-Terrorism Bill”, *Foreign Policy*. (03 October 2017)

Ellis Clare, Pantucci Raffaello, Zuijdewijn Jeanine de Roy van, Bakker Edwin, Gomis Benoît, Palombi Simon and Smith Melanie, “Lone-Actor Terrorism: Analysis Paper” (Royal United Services Institute 2016)

EUROPOL web site, https://www.europol.europa.eu/publications-events/main-reports/tesat-report (Accessed 18 July 2022).

“European Union Terrorism Situation and Trend report 2015”, (European Police Office 2015)

Federal Bureau of Investigation web site, available at https://www.fbi.gov/investigate/terrorism (Accessed 08 October 2020).

“Federal Bureau of Investigation Homegrown Violent Extremist Mobilization Indicators Booklet”, (2019), available at https://www.dni.gov/files/NCTC/documents/news_documents/NCTC-FBI-DHS-HVE-Mobilization-Indicators-Booklet-2019.pdf, (accessed 20 October 2021)

Feldman Matthew, “Comparative Lone Wolf Terrorism: Toward a Heuristic Definition”, *Democracy and Security* 9(3) (2013), pp.270-286;

Feve Sebastien, Bjornsgaard Kelsey, “Countering Lone-Actor Terrorism Series No. 3”, (Royal United Services Institute for Defence and Security Studies Lone-Actor Terrorism Database Workshop 2016)

“France to Deploy Soldiers after Spate of Attacks, *BBC*, (23 December 2014), available at https://www.bbc.com/news/world-europe-30586798 (accessed 25 March 2021)

“Frankfurt Airport Shooting may have Islamist Link, Say Police”, *The Guardian,* (03 March 2011), available at https://www.theguardian.com/world/2011/mar/03/frankfurt-airport-shooting-islamist-link? (accessed 25 March 2021)

“French police search home of man suspected of driving into soldiers”, *The Guardian*, (09 August 2017), available at https://www.theguardian.com/world/2017/aug/09/paris-police-hunt-driver-hit-soldiers-on-patrol-levallois-perret (accessed 08 October 2020)

Gill Paul, Horgan John and Deckert Paige, "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists" *Journal of Forensic Sciences* 59(2) (2014), pp.425-435.

Global Terrorist Groups Exploit Mentally ill People to Carry Out Attacks: Experts", The Straits Times, (12 May 2016), available at https://www.straitstimes.com/world/global-terrorist-groups-exploit-mentally-ill-people-to-carry-out-attacks-experts (accessed 25 March 2021)

Goldman Adam, "Why Didn't the F.B.I. Stop the New York Bombing?" (21 September 2016). Available at https://www.nytimes.com/2016/09/22/us/fbi-terror-ahmad-khan-rahami.html (Accessed 10 October 2020)

Gruenewald Jeff, Freilich Steven, Chermak Joshua, "Distinguishing 'Loner' Attacks from Other Domestic Extremist Violence A Comparison of Far-Right Homicide Incident and Offender Characteristics", *American Society of Criminology Criminology & Public Policy* 12(1) (2013), pp.65-91.

Gruenewald Jeff, Pridemore William, "A Comparison Of Ideologically-Motivated Homicides from the New Extremist Crime Database and Homicides from the Supplementary Homicide Reports Using Multiple Imputation by Chained Equations to Handle Missing Values", *Journal of Quantitative Criminology*, 28(1) (2012), pp.141-162.

Hafızoğulları Zeki, Kurşun Günal, "Türk Ceza Hukukunda Örgütlü Suçluluk", *TBB Dergisi*, (71) (2007), pp.25-80.

Hamm Mark, Spaaij Ramon, "Lone wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies", (U.S. Department of Justice 2015);

Hamming Tore, "Jihadi Competition and Political Preferences", *Perspectives on Terrorism*, 11(6) (2017), pp.63-88.

Hofmann David, "How 'Alone' are Lone-Actors? Exploring the Ideological, Signaling, and Support Networks of Lone-Actor Terrorists, *Studies in Conflict & Terrorism*, 43(7) (2018)

Holt Thomas, Freilich Joshua, Chermak Steven, Mills Colleen and Silva Jason, "Loners, Colleagues, or Peers_ Assessing the Social Organization of Radicalization", *American Journal of Criminal Justice*, 22(1) 2018, pp.83-105.

Horgan John, Gill Paul, Bouhana Noemie, Silver James and Corner Emily, "Across the universe? A Comparative Analysis of Violent Behavior and Radicalization Across Three Offender Types with Implications for Criminal Justice Training and Education", (National Institute of Justice 2016)

Jenkins Brian, "Stray Dogs and Virtual Armies Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11", (RAND 2011)

Jensen Richard, "The Pre-1914 Anarchist 'Lone Wolf' Terrorist and Governmental Responses", *Terrorism and Political Violence*, 26(1) (2014), pp.86-94.

Joint Publication 3-26 Counterterrorism", (U.S. Army 2009)

Kaplan Jeffrey, “Leaderless Resistance”, *Terrorism and Political Violence,* 9(3) (1997), pp.80-95.

Kaplan Jeffrey, Lööw Helene and Malkki Leena, “Introduction to the Special Issue on Lone Wolf and Autonomous Cell Terrorism”, *Terrorism and Political Violence* 26(1) (2014), pp.1-12.

“Leytonstone knife attack: man convicted of attempted murder”, *The Guardian*, (08 June 2016), available at https://www.theguardian.com/uk-news/2016/jun/08/leytonstone-knife-attack-man-convicted-of-attempted (accessed 16 October 2021).

Lia Brynjar, “Al-Suri’s Doctrines for Decentralized Jihadi Training – Part 1”, *Terrorism Monitor*, 5(1) (2007), available at https://jamestown.org/analyst/brynjar-lia/ (Accessed 15 May 2020)

Lindekilde Lasse, Bertelsen Preben and M Stohl ichael. “Who Goes, Why, and With What Effects: The Problem of Foreign Fighters from Europe”, *Small Wars and Insurgencies*, 27(5) (2016), pp.858-877.

“Man Arrested in French Car Attack had Radical Beliefs”, *The Washington Times*, (23 August 2017), available at https://www.washingtontimes.com/news/2017/aug/23/man-arrested-in-french-car-attack-had-radical-beli/ (accessed 20 March 2021)

Malthaner Stefan, Waldmann Peter, “The Radical Milieu_ Conceptualizing the Supportive Social Environment of Terrorist Groups”, Studies in Conflict & Terrorism, 37(12) (2014) pp.979-998

Marchment Zoe, Bouhana Noémie and Gill Paul, “Lone Actor Terrorists: A Residence-to-Crime Approach”, *Terrorism and Political Violence*, 32(7) (2018), pp.1-16.

Mccauley Clark, Moskalenko Sophia and Van Son Benjamin, “Characteristics of Lone-Wolf Violent Offenders: A Comparison of Assassins and School Attackers”, *Perspectives on Terrorism* 7(1) (2013), pp.4-24.

Meloy J. Reid, Gill Paul, “The Lone-Actor Terrorist and the TRAP-18”, *Journal of Threat Assessment and Management*, 3(1) (2016), pp.37–52.

Meloy J. Reid, Yakeley Jessica, “The Violent True Believer as a ‘Lone Wolf’ Psychoanalytic Perspectives on Terrorism”, *Behavioral Sciences and the Law*, 32(3) (2014), pp.347–365.

Morton Jesse, Silber Mitchell, “NYPD vs. Revolution Muslim: The Inside Story of the Defeat of a Local Radicalization Hub”, *CTC Sentinel*, 11(4) (2018), p.5.

Mueller Robert, “War on Terrorism”, (Testimony before the Select Committee on Intelligence of the United States Senate 2003), https://archives.fbi.gov/archives/news/testimony/war-on-terrorism (Accessed 12 November 2020)

Nesser Petter, “Single Actor Terrorism: Scope, Characteristics and Explanations”, *Perspectives on Terrorism* 6(6) (2012), pp.61-73.

Nesser Petter, Anne Stenersen and Emilie Oftedal, “Jihadi Terrorism in Europe: The IS-Effect”, *Perspectives on Terrorism*, 10(6) (2016), pp.3-24.

"Notre Dame Attacker 'Pledged Allegiance to IS in Video'", (07 June 2017), France24, available at https://web.archive.org/web/20170719031955/http://www.france24.com/en/20170607-notre-dame-attacker-pledged-allegiance-video, (accessed 20 March 2021).

Pantucci Raffaello, "Developments in Radicalisation and Political Violence A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists", (King's College International Centre for the Study of Radicalisation and Political Violence 2011)

"Paris attacks: Who were the attackers?", *BBC*, (27 April 2016), available at https://www.bbc.com/news/world-europe-34832512 (accessed 16 October 2021).

"Paris Knife Attacker was Known to Counter-Terrorism Police", (13 May 2018), *The Guardian,* available at https://www.theguardian.com/world/2018/may/13/paris-knife-attacker-khamzat-azimov-known-to-counter-terrorism-police (Accessed 08 October 2020).

"Paris Police Killings: Minister Calls for 'Automatic Alerts'", *BBC*, (07 October 2019), available at https://www.bbc.com/news/world-europe-49959827 (accessed 25 March 2021).

Patton Christina, Fremouw William. "Examining 'Suicide by Cop': A Critical Review of the Literature, *Aggression and Violent Behavior* (27) (2016) pp.107–120.

Phillips Peter, Pohl Gabriela, "Economic Profiling of the Lone Wolf Terrorist: Can Economics Provide Behavioral Investigative Advice?", *Journal of Applied Security*, 7(2) (2012), pp.151-177.

Schuurman Bart, Bakker Edwin, Gill Paul, and Bouhana Noemie, "Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis", *Journal Forensic Sciences*, 63(1) (2017), pp.1191-1200;

Schuurman Bart, Lindekilde Lasse, Malthaner Stefan, O'Connor Francis, Gill Paul, Bouhana Noemie, "End of the Lone Wolf: The Typology that Should Not Have Been", *Studies in Conflict & Terrorism*, 42(8) (2017), 771-778.

"Several injured in attack on train near Würzburg, southern Germany", *Deutsche Welle*, (18 July 2016), https://www.dw.com/en/several-injured-in-attack-on-train-near-w%C3%BCrzburg-southern-germany/a-19408848 (accessed 08 October 2021)

Smith Brent, Gruenewald Jeff, Roberts Paxton and Damphousse Kelly, "The Emergence of Lone Wolf Terrorism: Patterns of Behaviour and Implications for Intervention", *Sociology of Crime, Law and Deviance*, 20 (2015), pp.89–110.

Spaaij Ramon, "The Enigma of Lone Wolf Terrorism: An Assessment" *Studies in Conflict & Terrorism* 33(9) (2010), pp.854-870;

Spaaij Ramon, Hamm Mark, "Key Issues and Research Agendas in Lone Wolf Terrorism", *Studies in Conflict & Terrorism*, 38(3) (2015), pp.67-178.

Sutherland Jacqueline , "How Is ISIS Able to Commit Acts of Terror as It Loses Territory?", (08 November 2017), *The National Interest*, available at https://nationalinterest.org/feature/how-isis-able-commit-acts-terror-it-loses-territory-23111 (accessed 15 June 2021)

"Syria Releases the 7/7 Mastermind", *The Telegraph* (04 February 2012), available at https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9061400/Syria-releases-the-77-mastermind.html, (Accessed 20 May 2020).

Teich Sarah, "Trends and Developments in Lone Wolf Terrorism in the Western World an Analysis of Terrorist Attacks and Attempted Attacks" (IDC Herzliya International Institute of Counter Terrorism October 2013)

The Terrorist Radicalization Assessment Protocol-18 / TRAP-18.

The Threat from Solo Terrorism and Lone Wolf Terrorism", (Politiets Efterretningstjeneste Center For Terroranalyse 2011)

"UK Facing Most Severe Terror Threat Ever, Warns MI5 Chief", *The Guardian*, available at https://www.theguardian.com/uk-news/2017/oct/17/uk-most-severe-terror-threat-ever-mi5-islamist (Accessed 05 July 2021).

United Nations Security Council Resolution 2178", (2014), available at https://www.un.org/securitycouncil/s/res/2178-%282014%29 (accessed 03 October 2020);

Weimann Gabriel, "Lone Wolves in Cyberspace", *The Centre for the Study of Terrorism and Political Violence*, 3(2) (2012), pp.75-90.

E-DATR, 2022; 16 : 109-128
ISSN 1307 - 9190

Children Recruiting And Exploiting By Terrorist Groups

Zehra Eroğlu Can[1]

Abstract: *A large number of children are being trafficked by terrorist and violent extremist groups. Determining the childhood age limit for children exploited by terrorist organizations is important. Determining the boundary between childhood and maturity is a contentious issue. There are various points of contention over determining when childhood ends and adulthood begins. In international law "child" is defined as "every human being below the age of eighteen years." Terrorist Groups prefer recruiting children due to visibility and propaganda, economic considerations and effectiveness, easy control and tactical advantages. The methods of terrorist groups to recruit children could be summarized as, forcible recruitment, economic enticement, transnational recruitment, use of schools (education), propaganda and online recruitment. The children in terrorist groups face to extreme violence and as a result they could easily have physical and mental harm, so rehabilitation and reintegration programs are main milestones in their new life. Governments ought to support transnational and multidisciplinary cooperation to create and carry out programs taking care of instances of children having been presented to terrorist groups. Sustained reintegration activities involve deradicalization, re-education, reintegration and community outreach jurisdictions.*

Keywords: *Children, Recruitment, Terrorist Groups, Reintegration, Rehabilitation.*

[1] Zehra EROĞLU CAN, TGS, zseroglucan@gmail.com

1. Introduction:

Nearly all terrorist organizations from Asia to Africa look for recruiting children. In such regions it will getting difficult to save children from a landscape in which they could be exploited as couriers, spies, fighters and even suicide bombers. Political, economic problems and insecurity give safe havens for these groups for setting up their training camps, especially in border regions. These children can easily be radicalized using simple things like food, some money, or just candy. They are trained to carry out suicide attacks.

It is highly critical to make a clear definition of the child. Although there are different criminal responsibility ages in different countries, international law defines the people who are under 18 as “child”.

The unemployment, illiteracy, common poverty and deficiency of the rule of law could cause the recruitment and exploiting of children by terrorist groups. Terror groups have many ways to exploit children such as coercion, financial aid or proposing protected status for children or their family. The rising violence and insecurity in the world make it easy for terror groups to reach and convince the children. In some places such Syria and Afghanistan terrorist organizations offer two choices to families; giving some amount of money in every month or give one of their children. Families choose second one because of poverty and the reality of large families. In addition to this, family ties give another opportunity for recruitment: the child of terrorist become new member. Terrorist organizations can influence the education system in the regions under their control in such a way that they can train new members. This can be seen as another method for terrorist organizations to recruit children.

It is stated that terrorists exploit children because they can quickly gain the trust of potential victims. Terrorist organizations train children as suicide bombers, and it is often stated that the children exploited in this attack are not even aware of what they are doing.

The rehabilitation of formerly recruited children is another problematic issue. Due to lack of sufficient support for reintegration, these children could easily choose to return to terrorist groups. It is seen that in the studies carried out so far, a special approach for children exploited by terrorist organizations has not been revealed, and there is uncertainty about how these children will be reintegrated into society, especially when they are rescued from terrorist organizations. In this study it is

stated that rehabilitation and reintegration methods for adults are not suitable for children. It would be more beneficial to adopt an approach according to the age of the children, the time they spent in terrorist organizations, and the size and scope of the activities they participated in. The failure in the process of reintegration and rehabilitation may lead these children back to terrorist organizations. To sum up, the failure of countries and governments to develop a special program for these children may lead to the emergence of new and more radical terrorists. Besides, reintegrating children under the influence of terrorist groups such as DAESH into society and succeeding in keeping them away from radicalization may make DAESH lose its effect. However, the lack of a special regulation for these children in international law is one of the most important shortcomings.

2. Terms And Legal Regulations:

2.1. Definition of a Child:

Determining the childhood age limit for children exploited by terrorist organizations is important in many respects. Terrorist organizations generally prefer children because they can be persuaded more easily, they are punished less if they are caught, etc. In this regard it is highly important to define "who is child".

There are many matters of dispute about determining the beginning and end of childhood.

Although, the exploiting of children in armed conflicts is forbidden by international law many terror groups prefer to use them. According to international law "child" refers to a human being under the age of eighteen years but there are different age limitations e.g., the age of criminal responsibility, the age of sexual consent could be different in many countries. In 2007 the UN in the Paris Principles on the Involvement of Children in Armed Conflict defined children in combat as follows: "*Children in combat are defined as "any person below the age of 18 who is, or who has been, recruited or used by an armed force or armed group in any capacity, including but not limited to children, boys and girls, exploited as fighters, cooks, porters, spies, or for sexual purposes," according to the Principles on the Involvement of Children in Armed Conflict."* [2]

---

[2] Principles and Guidelines on Children Associated with Armed Forces or Armed Groups ("the Paris Principles"), at: https: www.icrc.org (accessed on 25 May 2021), p.7.

The United Nations (UN) Convention on the Rights of the Child describes a child as an individual under the age of 18.

In line with the Article 31 of the Turkish Penal Code:

"Children who are under the age of 12 when the conduct is committed are not criminally liable. These people cannot be criminally prosecuted, although child-specific safety measures might still be necessary.

There is no criminal liability for those who committed the act but were over the age of twelve but under the age of fifteen because they were unable to understand the conduct's legal significance and repercussions, or because their capacity to control their behavior was insufficiently developed. If the offense calls for aggravated life in prison, the defendant receives a sentence ranging from fourteen to twenty years, and if the crime calls for life in prison, the defendant receives a term ranging from nine to twelve years." (TCK artc.31)

Many factors such as cognitive abilities, emotional maturity and social development play role in the definition of a child. It is difficult for countries to determine a common legal stance on the exploiting of children by terrorist organizations because the criminal responsibility age and conscription varies due to the different cultures of the countries.

2.2. The Recruitment and Exploiting of Children by Terror Groups under International Law:

In an armed conflict, children are seen as easy targets not only for violence, but also for coercion and indoctrination, because of their young age they often do not have a pre-established value system, so children are more easily coerced and indoctrinated than adults. DAESH's exploiting children as a propaganda instrument and as militants has become quite common. Children have carried weapons, guarded strategic locations, arrested civilians, been subjected to sexual violence, forced marriage, and exploited in suicide bombings.

Although in the case of states there are some limits in international law regarding the age limit of child soldiers, in the case of terrorist organizations it is not possible to talk about such a limit on the members' age. Since the norms of international law are not binding for most terrorist organizations, it is possible to come across children exploited by terrorist organizations at almost any age.

Within the context of the European Union Agency for Law Enforcement Cooperation (Europol) estimation, since the start of the Syrian civil war in 2011, nearly 5,000 foreign fighters have traveled from Europe to Syria and Iraq. The United Nations is also urging states to bring children back from Syria. A large amount of them are children of DAESH terrorists in Iraq and Syria. According to U.N. humanitarian officials, about 62,000 people live in Al-Hol, the country's largest camp for refugees and displaced persons. [3]

Within the human rights perspective, Article 38(2) of the 1989 Convention on the Rights of the Child states, *"States parties shall take all practicable measures to ensure that persons under the age of 15 do not directly participate in hostilities*" and Article 38(3) "*requests States not to recruit children under the age of 15 into their armed* forces''. The Optional Protocol to the Convention on the Rights of the Child accepted in 2000 and it paved the way for the broadening the international law framework by raising the age for participation in hostilities to 18 (Article 1) and prohibiting the recruitment or exploiting of persons under the age of 18 in hostilities by armed groups (Article 4).[4] The African Union accepted the African Charter on the Rights and Welfare of the Child in 1999. It defines a child as anyone below the age of 18 without exception. International treaties also include recommendations on prevention and disarmament, demobilization and reintegration (DDR) efforts in traditional armed conflict, some of which are aimed at countering violent extremism of children, but additional international standards are required in these particular cases.

Some international documents that define the age of childhood could be seen in Additional Table 1.

---

[3] Russia Repatriates 34 Children from Camps in Syria", Daily Sabah, Apr 19, 2021, p.1.

[4] Nina H.B. Jørgensen," Children in Conflicts as Victims and Perpetrators? Reassessing the Debate on Child Soldiers in Light of the Involvement of Children with Terrorist Groups", (Questions of International Law, Jun 30, 2019) p.11.

Additional Table:1
International Law and the Age of Childhood[5]

<table>
<tr><th>ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT</th><th>GENEVA CONVENTION AND ADDITIONAL PROTOCOLS</th></tr>
<tr><td>Established 1998.
122 States Ratified.
Age of Child: Under 15.
Recruiting a child to actively participate in international or domestic hostilities is a war crime.
The forced transfer of children from one group to another is genocide.
Rape, sex slavery and forced pregnancy are crimes against humanity and war crimes in the conflict.</td><td>Established 1949.
196 States Ratified Convention IV.
Additional Protocol I Ratified by 174.
Age of Child: Under 15.
Children under 15 years of age are prohibited and use is not recommended if under 18 years of age are directly involved in the conflict.
Children have the right to food, medical care, protection, and family reunification where possible.
If prosecuted, separate accommodation and exempt from the death penalty if under 18 years old.</td></tr>
<tr><th colspan="2">OPTIONAL PROTOCOL TO THE CONVENTION ON THE RIGHTS OF THE CHILD ON THE INVOLVEMENT OF CHILDREN IN ARMED CONFLICT</th></tr>
<tr><td colspan="2">Established 2000.
162 States ratified.
Age of Child: Under 18.
Playing a direct role in the conflict is prohibited for anyone under the age of 18 in the armed forces and groups, but the armed forces may enlist 16- and 17-year-olds if they volunteer, with appropriate parental consent and proof of age.
Purposes for full reintegration, with States giving the necessary funding.</td></tr>
<tr><th>THE PARIS COMMITMENTS</th><th>THE PARIS PRINCIPLES</th></tr>
<tr><td>Established 2007.
Summary of Paris Principles.
100 States Ratified
Age of Child: Under 18.
Address the harms of engaging in conflict through technical support and funding.
Committed to addressing the imbalance in helping girls in conflict.</td><td>Established 2007.
100 States Ratified
Age of Child: Under 18.
Prohibit children from confrontation in active and supportive roles such as cooks, porters, messengers, spies, and sexual partners.
Prevention and GDR guidelines; financial, educational and community opportunities.
No death penalty, life imprisonment, or international prosecution for persons under 18.
Children who run away are not deserters. No torture, voluntary search for truth.</td></tr>
</table>

[5] Noman Benotman & Nikita Malik, “The Children of Islamic State”, (The Roméo Dallaire Child Soldiers Initiative, Quilliam 2016), p.13.

3. The Advantages of Exploiting Children By Terrorist Organizations

Children are seen as the next generation of DAESH. Child warriors are defined by the organization as "Cubs of the Caliphate". According to a study conducted in early 2016, it was determined that DAESH enslaved 3500 people in the areas it controlled, and 800 to 900 children were kidnapped in Mosul alone to be raised as terrorists.[6] Since 2015, children's training camps have been opened for their education, and in these camps, they have been provided with training in many fields from suicide attacks to armed attacks and to take active duty. In the published propaganda videos, children dressed in camouflage are seen with their leaders, who command them. [7]

The Advantages of Using Children by Terrorist Groups could be summarized as follows:

- Visibility and propaganda:

Terrorist groups and violent extremists frequently exploit children to increase their awareness, as evidenced by Boko Haram and DAESH propaganda. The photographs are designed to shock the public while also demonstrating the group's power and cruelty.

- Economic considerations and effectiveness:

Terrorist groups and violent extremists, as well as armed groups in general, gain from significant financial advantages when recruiting children. Children are often paid less (if at all) and need less food to survive, whether exploited in a support or warrior role. Parallel to this, combat has evolved, and the prevalence of small guns, in particular, has narrowed the effectiveness difference.

- Control:

Children are more easily intimidated and controlled than adults, both physically and intellectually. In addition to this, being deprived of adequate educational opportunities and unemployment are also important factors in the easy deception of children by terrorist groups.

---

6 "Kuruluşundan Eylem Yöntemlerine DEAŞ Terör Örgütü", (TERAM (Terörizmle ve Radikalleşme ile Mücadele Araştırma Merkezi), 17 Temmuz 2020), p. 5

7 Ibid.

- Tactical advantages:

Children are increasingly being exploited as spies to deliver messages, transport equipment and make suicide attacks. The reasons for this are often pragmatic: young people have a limited understanding of the risk they face and are therefore less worried about it.[8]

4. The Methods Used By Terrorists To Recruit Children

It is stated that there are six phases in children's social adaptation into DAESH: Seduction, Schooling, Selection, Subjugation, Specialization, and Stationing.[9]

Seduction: Initial exposure to ideas, standards, and practices through advocacy, offsite participation in public events, and indirect outreach to employees.

Schooling: Routine, direct exposure to personnel, accompanied by heavy indoctrination.

Selection: Employers focus attention, select skills, and prepare for military training or other roles.

Subjugation: Physical and psychological brutality through comprehensive training, separation from family, wearing of uniforms, and deeper commitment through acts of loyalty, sacrifice, and discipline; the emergence of unity through shared challenge. Specialization: Professional advancement and exposure to specialized training. Stationing: Assign and deploy roles; including participation in public events to recruit new members.[10]

The methods used by terrorists to recruit children could be summarized as follows:

- Forcible recruitment (Coercion):

Violent extremist and terrorist groups are primarily participated in the forcible and usually brutal recruitment of great numbers of children. Children can be kidnapped, threatened or bought from human traffickers. Like street children, children living in poverty and without parental care are particularly vulnerable to forced conscription.

---

8 "Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System", (United Nations Office on Drugs and Crime Vienna, 2017), p.11.

9 John Horgan et al., "From Cubs to Lions: A Six Stage Model of Child Socialization into the Islamic State", "From Cubs to Lions: A Six Stage Model of Child Socialization into the Islamic State", Studies in Conflict&Terrorism, Vol. 40 (7), (2016), p.11

10 Ibid., p.12.

Under some circumstances, recruitment through connections with group and community leaders plays a substantial role. In this case, members of families and communities can encourage children to participate in the armed groups.

In DAESH, children between the ages of 5 and 10 in religious education camps, while children between the ages of 10 and 15 receive military training.[11] Media reports indicate that children were beaten, tortured, raped if they refuse to obey DAESH orders. In addition to this, local tribes reportedly forced families to send their children to DAESH in some cases. The families who do not allow DAESH to take their children asserted that the children were forced to participate in conflict.

DAESH prefers more indirect and systematic coercion. People, especially children, are forced to join organizations out of fear. DAESH continues to cruelly punish and kill people who do not comply with its code of conduct or who believe that it is contrary to its ideology.[12]

- Economic enticement:

In some cases, terrorist groups may propose payment, food, shelter and protection, encouraging loyalty.[13]

In the past, the payment of wages by armed groups was seen as a vital factor in the recruitment of children, as was the case often with children in the DAESH. The exceptionally excessive wages paid with the aid of the DAESH encouraged children and their families in a tough and conflict-torn economic environment.

- Transnational recruitment:

The transnational characteristic of terrorism and violent extremism facilitates the emergence of transnational recruitment and participation of children in foreign terrorist fighters. Some children who joined terrorist organizations across borders did so by themselves, some traveled with their families or adult relatives, while others were forcibly abducted and then crossed borders as part of participating in violent extremist organizations. Some groups have developed comprehensive recruitment strategies, including a lot of recruitment styles suitable for different situations.

---

11 Benotman & Malik, “The Children of Islamic State”, p.34

12 Ibid., p.32-33.

13 Lorne L.Dawson, “A Comparative Analysis of the Data on Western Foreign Fighters in Syria and Iraq: Who Went and Why?” (ICCT Research Paper, February 2021), p.40.

- Use of schools (Education):

Terrorist groups and violent extremists try to extend their power through schools, which are used as a forum for children to be indoctrinated.

First of all, socialization involves interacting with children, often in public places or mosques, and promoting contact with DAESH by providing free toys and sweets, or opportunities holding the DAESH flag and in some cases, weapons. At this phase, the children are exposed to DAESH ideology and are attracted by the military success of the so-called Caliphate.

- Propaganda:

The group develops a precise communication strategy aimed at emphasizing the benefits of taking part in the group or generating empathy. Being a member of a group could present status and prestige, elegant uniforms and weapons. It could be seen as a chance for gaining power, particularly for children who have no educational opportunities or jobs. DAESH also frequently pays attention to "victimization" and uses images showing "enemy crimes" to release anger, arouse sympathy for the injured or killed, and create a desire for revenge. In addition to this, such groups use some interactive media tools such as computer games and cartoons to distribute their information. The aim of glorifying terrorist attacks could be seen at the core of these materials.

Taking part in terrorist groups such as DAESH ensures children a degree of satisfaction because they are needed and appreciated. Furthermore, under the indistinct conditions of conflict, membership of DAESH gives a sense of power. As a result of ongoing wars, the majority of the people feel exhausted and powerless. At that point, joining a terrorist group could be seen as a solution to their problems.[14]

In a video released in February 2015, 80 youngsters, some as young as five years old, were seen dressed in camouflage, standing in formation, and engaged in military drills with rifles. These kids were supposedly taught how to decapitate people and wield AK-47 rifles.[15]

---

[14] Ibid., p.35.

[15] Mia Bloom, "Weaponizing the Weak: The Role of Children in Terrorist Groups", (Washington & Lee Public Legal Studies Research Paper Series, No. 2019-06, Chapter 09, January 14, 2019), p.3

- Online recruitment:

The use of online communication is called as a new way of disseminating extremism and terrorism propaganda. It is useful for conveying ideology of terror groups all over the world and children are subjected to such activities as active internet users.[16] The terrorist groups learn to use this instrument gradually. While social media platforms such as emails, chat rooms, mail groups, electronic products, message boards and other applications become popular, terrorist groups adapt their recruitment tactics according to these new platforms. However, these new recruitment methods cause a tailored recruitment approach.

One of these methods can be defined as "modification", which relies on the perpetrator to understand the individual's interests in order to adapt to the method and establish a relationship of trust. The other technique could be called as "targeted advertising": By tracking the online behavior of internet users, a group can identify those groups that are vulnerable to its propaganda and customize the narrative according to its target audience.[17]

With the increased usage of children, they have been deployed as soldiers, human shields, couriers, spies, and guards. Boys are assigned specialized tasks and stations after attending DAESH schools and learning military skills in its training camps. These usually entail acts that children are better suited to.

Girls receive a domestic education in which they learn how to care for their husbands' needs, raise their children within the conformity with the DAESH's ideology. DAESH doctrine, known as the "*flowers and pearls of the caliphate*," has very precise requirements for girls: they must be properly covered, disguised, and never leave the house unless under extraordinary circumstances.[18]

With its territorial grip in Iraq and Syria slipping away, it is unclear whether DAESH will be able to continue its recruitment efforts indefinitely. DAESH ran a slick, modern social media campaign from its Mosul and Raqqa centers for several years, distributing messages in as many as 25 languages across a variety of open Application Programming Interface (API) and encrypted social media platforms (such as Twitter, Kik, Pinterest, WhatsApp, Viber).[19]

---

16 Dolunay Şenol, Sezgin Erdem, Elif Erdem, "IŞID: Küresel bir Terör Örgütü", Fırat Üniversitesi Sosyal Bilimler Dergisi, 26 (2) (2016), p.286.

17 "Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System", p.13.

18 Bloom, "Weaponizing the Weak: The Role of Children in Terrorist Groups", p.1

19 Ibid., p.2.

5. The Status of Children Associated With Terrorist Groups

Except for the general effects of war on every human, it affects children in many different ways. These effects include not only physical harm (death, injury, disability or illness) but also psychological harm. The drawn-out presentation and desensitization to savagery that children involvement amid war causes long term injury, which disables the mental and ethical advancement of the children. Moreover, the insufficiency of foundation like schools and healing centers hinders get to instruction and healthcare, which can have a negative affect both within the short and the long-term. As an example, more than 800,000 people were killed in a three months period in Rwanda in 1994. According to a study which focuses on this event, it is highlighted that 95.9 percent of children saw savagery, 87.5 percent faced to dead bodies or body parts and 69.5 percent were witnessed slaughtered or injured people. Although a long time passed, the ongoing effects could be seen on those who have survived.[20]

In this regard, the effect of war on children can be complex. However, what is obvious is that the negative results can take years to remove. Agreeing to UNICEF, more than 16 million babies were born in strife zones in 2015, a figure that underscores the defenselessness confronted by expanding numbers of children.[21]

The children formerly associated with terrorist groups do not only face to a trauma but also other post-conflict fears rage from revenge attack, re-recruitment, stigmatization, deep poverty and family violence. As a result, these children create some solutions for their traumas, as an example they refuse to think about their wartime experiences. At that point the role of their family and friends become highly vital for coping with the emotional stress of their experiences.

DAESH is thought to have transnational potential thanks to its indoctrination and weaponization of children. This is, DAESH's ability to withstand and survive territorial defeat.[22] For this reason, reintegrating these children under the influence of DAESH into society and succeeding in keeping them away from radicalization may make DAESH lose its effect.

---

20 Benotman & Malik, "The Children of Islamic State", p.46

21 Ibid.

22 Asaad Almohammad, "ISIS Child Soldiers in Syria: The Structural and Predatory Recruitment, Enlistment, Pre-Training Indoctrination, Training, and Deployment", (ICCT Research Paper, February 2018), p.2.

5.1. An End or New Beginning (Rehabilitation and Reintegration)

Whatever their role the children in terrorist groups confront extreme violence and as a result they could easily have physical and mental harm. It could be seen that many very young members in terror groups and DAESH in particular. For example, the photograph shows a 7 years old child holding up a decapitated head of a victim of DAESH. The other example is a video that includes 4 years of child detonating a car-load of explosives in January 2016.[23]

Due to the poor life conditions of Syrian refugee camps, the immediate ways to save children from these problems, should be priority for in international community.

Despite growing public awareness and efforts to repatriate children, national actions are limited and ad-hoc. Separation from their DAESH-affiliated parents is another concern raised by children repatriation. Separation could aggravate pain suffered by children, despite the fact that DAESH-affiliated parents have put their children in danger by traveling to DAESH territory. This emphasizes the importance of evaluating the methods of repatriation and rehabilitation requirements for children on an individual basis.[24]

The actions and methods used by states parties for the children repatriated from Syria and Iraq should be in conformity with the principles of the UN Convention on the Rights of the Child (CRC).

Firstly, according to the regulations in international law, states have obligations to accept all possible measures to hinder the recruitment of the children under 18 years old by terrorist groups.

Secondly in line with the responsibilities derive from international law, states should provide rehabilitation to the children who have recruited by terror groups. The states should be treated these children according to their rights, needs and dignity in line with the obligations stem from the CRC.[25]

Thirdly, because of the possibility of becoming the victims of trafficking, these children could need special protection under the international law. These children could be forced to work for the trafficker or others. Their duties could

---

[23] John Horgan et al., "From Cubs to Lions: A Six Stage Model of Child Socialization into the Islamic State", p.8.

[24] Joana Cook and Gina Vale, "From DAESH to 'Diaspora': Tracing the Women and Minors of Islamic State", International Centre for the Study of Radicalization, Department of War Studies, King's College, (2018), p.10.

[25] UN General Assembly Resolution A/RES/70/291

contain anything from banded or forced labor to commercial sexual exploitation. International regulations make it clear that no children could be punished, prosecuted or threatened for being a member of an armed group.[26]

The treatment of children should be consistent with the age, role and the membership consent of the children in a terrorist group. Besides, these treatments should pave the way for the reintegration of the children to the society.[27] According to the CRC every child has a right to acquire a nationality. The Convention on the Reduction of Statelessness bans States from depriving a person of nationality if doing so would render the person stateless and everyone has a right to enter their own country.[28] Finally, children could not be detained due to their or their parents' immigration status and no children should be subjected to preventive or administrative detention for counter-terrorism aims.[29]

Despite the obligations arising from international law, many differences are observed in the approaches of states to children who have connections with terrorist organizations and their policies towards these people.

The returned children face to many rehabilitation processes in their home countries. As of July 2019, 403 children had returned to Kazakhstan from Iraq and Syria, and nearly 41 children returned to Tajikistan for two-year period.[30] Denmark has preferred its "Aarhus model" for the returnees' reintegration. Aarhus model includes cooperation and coordination between social workers, police and religious groups. Nevertheless, this model is focused on the children groomed by the terror groups to commit criminal offences.[31]

Rehabilitation programs can fail when the underlying policy is not well understood. Programs that are not well thought out, that do not take all factors into account, are likely to fail. In other words, the disadvantages of such programs could be

---

26 Principles and Guidelines on Children Associated with Armed Forces or Armed Groups ("the Paris Principles"), principle 8.7.

27 Convention on the Rights of the Child, at: https: //www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed on 05 May 2021), Article 40(1).

28 Convention on the Reduction of Statelessness 1961, at: https://www.unhcr.org/un-conventions-on-statelessness.html (accessed on 04 May 2021) Article 8(1)

29 Convention on the Rights of the Child, at: https: //www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed on 05 May 2021), Articles 3(1) and 37.

30 Russia's Repatriation of ISIS Members", Foreign Policy Research Institute, 12 April 2019, at: https://www.fpri.org/article/2019/04/russias-repatriation-of-isis-members/ (accessed on 24 May 2021).

31 Child Rights International Network (CRIN), "Bringing Children Home: A children's Rights Approach to Returning from ISIL", 28 Jan 2020, at: https://reliefweb.int/report/syrian-arab-republic/bringing-children-home-childrens-rights-approach-returning-isil (accessed on 27 May 2021), p.3.

more than their advantages. In this regard, policy tools need to be accurately and logically aligned with the objectives of the program.[32]

5.2. The Attitude of Other Actors (Governments or Home Countries)

Governments ought to support transnational and multidisciplinary cooperation to create and carry out programs taking care of instances of children having been presented to DAESH narratives. Prior to setting out on the improvement of any strategies or projects to help kids that have been living heavily influenced by DAESH, it should be directed a few appraisals to assess the degree to which the children had been exposed to the narratives of DAESH, just as the degree to which those narratives had been internalized. It is significant to keep away from worsening the situation by calling individuals and ideas as 'extremists' or 'terrorists.' This will only deepen the gap between communities and likely decline the possibility of establishing trust and dialogue with these individuals. In this context, public awareness about the government's repatriation, rehabilitation and reintegration policies is important to ensuring the public is equipped with accurate and up-to-date information.

Deradicalizing children from DAESH who have known no alternate lifestyle, and who have gone through serious physical and mental injury, will be a thorough interaction. It will be essential to initially decide if kids are joining voluntarily, or with their families. Another determining factor is age, regardless of whether the children being referred to join DAESH in their adolescent years or at a more youthful age. As such any course of appraisal ought to perceive the level of office and free idea behind radicalization, and in doing as such decide how much children are revolutionaries or confused.

Taking children back to normal life will be troublesome, and it is prescribed appraisal offices to assess the degree of every child's radicalization dependent upon the situation, and to offer ways for reintegration, trailed by a broad time of help from a local area organization. Tracking the children with proposals from the appraisal group will likewise assist with figuring out which kids can start deradicalization programs without legal procedures, and help in fair treatment of ceaseless evaluation and assessment.

---

[32] Tinka Veldhuis, "Designing Rehabilitation and Reintegration Programs for Violent Extremist Offenders: A Realist Approach", (ICCT Research Paper, March 2012), p.17.

The reintegration process involves four steps such as; Deradicalization, Re-Education, Reintegration and Community Outreach:

Deradicalization: Preventing radicalization can disperse and dissolve extremist ideology and understanding. Also, radicalization in prisons and the problem of returning terrorists is addressed through prevention programs.[33]

Deradicalization methodology will mean to rescue children once again from the way of life they have embraced, with adequate thoughtfulness regarding the physical and mental injury brought about by struggle. Measures ought to have a "values-based" educational plan which re-teaches kids with public qualities, gives philosophical and philosophical recalibration, and scholarly, social, and enthusiastic help.

National deradicalization operations must consider possible DAESH returnees and the people who have extremist ideologies in state borders, in conflict areas and in other foreign theaters. All parties must be encouraged and adequately supported to integrate children in all post-conflict legal, judicial, and recovery and transitional justice processes.

Re-Education: The aim of this stage is destroying the DAESH's credibility and changing these narratives with the positive ones. The endeavors would delegitimize DAESH's philosophy, and discredit the outrageous thoughts of nationhood and strict influence that children would have encountered in their past schooling framework in DAESH. It would consequently be imperative to deconstruct the instructive and scholarly parts of DAESH's educational program, and make another educational plan to uproot this. Besides this, all children will ultimately require help with getting a new line of work, a school, and a home, just as significant enthusiastic help and elective references and perspectives.

Reintegration: The majority of crafted by the organization will be on long haul reintegration of children in their networks. While children create new personalities and look for another feeling of having a place, it is basic they discover acknowledgment and freedoms to feel of strengthening and self-esteem inside a peaceful way of life. Instructive and business openings can help with assisting kids with focusing on their new way of life, and whenever the situation allows, ought to use the remarkable abilities of the children, and move them to occupations or instructive jobs inside the common state.

---

[33] Andrew GUNN ve Ahmet DEMİRDEN, "Radikalleşmenin Önlenmesi& Terörizm Olgusu", (Polis Akademisi Yayınları:72, Rapor No: 24, Haziran 2019), p.15.

Community Outreach: Policy can't direct community perspectives that guarantee fruitful reintegration, which can be particularly difficult as returning unfamiliar contenders frequently come from minority foundations inside their networks. Infrastructure is therefore anticipated to cooperate with return and reintegration efforts at both the global and local level, depending on the planned network. They ought to draw in networks for input with respect to children and include them in joint drives.[34]

Recently, government agencies in Turkey have been trying to design studies for removing returning DAESH members from extremist ideology and violence. People who are considered to be a threat are monitored and trying to deter those deemed to be turning to DAESH by using short-term detentions.[35]

6. Conclusion and Recommendation

The status of children in Iraqi and Syrian displacement camps and repatriated children affected by DAESH is a significant issue. It is critical to reverse the indoctrination process and support reintegration into education systems that provide specialized assistance to children on positive self-identification and social coherence. These are essential for breaking a perilous cycle of violent extremism and protecting children, which is a fundamental human right.

Policies and rehabilitation methods to be developed for children rescued from terrorist organizations by states are factors that will determine not only the future of these children, but also the future of countries and terrorist organizations from which they left. The issue of how to tackle the cases of DAESH-affiliated children is a critical problem. Societies are afraid of people that have formerly been affiliated with DAESH, even children, because they think that rehabilitation and reintegration attempts might be useless at reversing the radicalization process. Governments should definitely describe the periods for rehabilitation and reintegration of DAESH-affiliated children and give opportunities for the community to contribute to the formation of policies. After that the path of unification and peace could start and all children could be protected.

---

34 Benotman & Malik, "The Children of Islamic State", p.65.

35 International Crisis Group, "IŞİD'e Katılıp Dönen Türkiye Vatandaşları: Mevcut Yaklaşımları Geliştirmek", (Avrupa Raporu, N°258, 29 Haziran 2020), p.ii.

Although the lessons and practices associated with DDR programs are well established, they are usually for child soldiers. There is a need to adapt DDR programs to children recruited by terror groups. It might be anticipated a similar dynamic to wrap future talks almost how to reply to DAESH's children, but given the emerging spectacle of a potential future era of combatants, comprehending this could be a genuine concern. In the implementation of such programs, security organizations, prison staff, religious scholars, social opinion leaders, among various stakeholders, including psychologists and specialized NGOs coordination is important. Such programs are criticized in some countries due to diverting them from their original purpose due to targeted stigmatization of the environment, instrumentalized by the state for monitoring activities, or the use of social programs for counter-terrorism purposes.

The social reintegration of children should contain health and psychosocial recuperation and support; instructional and vocational opportunities; returning to family and community life. These components are interrelated, and failing to address any of them will almost certainly have a detrimental effect on the success of the whole reintegration process. Children's programs and services should adopt a comprehensive approach, including the children's unique needs and rights, as well as the expectations and demands of families and communities, as well as the features of the setting in which the reintegration process will take place. Reintegration measures ought to take into consideration the specific settings of children, including children in cross-border situations, children facing release from terrorist or violent extremist groups and children in contact with the justice system as alleged offenders.

If the international community is to have any hope of reintegrating those children who survive and leave DAESH, one thing is certain: it will take a degree of coordination and inventiveness that has never been seen before in any deradicalization campaign.

Bibliography

1. Almohammad, Asaad, "ISIS Child Soldiers in Syria: The Structural and Predatory Recruitment, Enlistment, Pre-Training Indoctrination, Training, and Deployment", (ICCT Research Paper, February 2018).
2. Benotman, Noman & Malik, Nikita, "The Children of Islamic State", (The Roméo Dallaire Child Soldiers Initiative, Quilliam 2016).
3. Bloom, Mia, "Weaponizing the Weak: The Role of Children in Terrorist Groups", (Washington & Lee Public Legal Studies Research Paper Series, No. 2019-06, Chapter 09, January 14, 2019).
4. Convention on the Reduction of Statelessness 1961, at: https://www.unhcr.org/un-conventions-on-statelessness.html (accessed on 04 May 2021).
5. Convention on the Rights of the Child, at: https: //www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed on 05 May 2021).
6. Cook, Joana and Vale, Gina, "From DAESH to 'Diaspora': Tracing the Women and Minors of Islamic State", International Centre for the Study of Radicalization, Department of War Studies, King's College, (2018).
7. Child Rights International Network (CRIN), "Bringing Children Home: A children's Rights Approach to Returning from ISIL", 28 Jan 2020, at: https://reliefweb.int/report/syrian-arab-republic/bringing-children-home-childrens-rights-approach-returning-isil (accessed on 27 May 2021).
8. Dawson, Lorne L., "A Comparative Analysis of the Data on Western Foreign Fighters in Syria and Iraq: Who Went and Why?", (ICCT Research Paper, February 2021).
9. GUNN, Andrew ve DEMİRDEN, Ahmet, "Radikalleşmenin Önlenmesi&Terörizm Olgusu", (Polis Akademisi Yayınları:72, Rapor No: 24, Haziran 2019).
10. "Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System", (United Nations Office on Drugs and Crime, Vienna, 2017).
11. Horgan, John G., Taylor, Max, Bloom, Mia and Winter, Charlie, "From Cubs to Lions: A Six Stage Model of Child Socialization into the Islamic State", Studies in Conflict&Terrorism, Vol. 40 (7), (2016), pp.645-664.
12. International Crisis Group, "IŞİD'e Katılıp Dönen Türkiye Vatandaşları: Mevcut Yaklaşımları Geliştirmek", (Avrupa Raporu, No.258, 29 Haziran 2020).
13. Jørgensen, Nina H.B.," Children in Conflicts as Victims and Perpetrators? Reassessing the Debate on Child Soldiers in Light of the Involvement of Children with Terrorist Groups", (Questions of International Law, Jun 30, 2019).
14. "Kuruluşundan Eylem Yöntemlerine DEAŞ Terör Örgütü", (TERAM (Terörizmle ve Radikalleşme ile Mücadele Araştırma Merkezi), 17 Temmuz 2020).

15. Principles and Guidelines on Children Associated with Armed Forces or Armed Groups (“the Paris Principles”), at: https: www.icrc.org (accessed on 25 May 2021).
16. “Russia’s Repatriation of ISIS Members”, Foreign Policy Research Institute, 12 April 2019, at: https://www.fpri.org/article/2019/04/russias-repatriation-of-isis-members/ (accessed on 24 May 2021).
17. “Russia repatriates 34 children from camps in Syria”, Daily Sabah, Apr 19, 2021.
18. Spyra, Stephanie Elisabeth, “Cubs of the Caliphate-How to Deal with a New Generation of Child Soldiers?”, Defense against Terrorism Review DATR, Vol. 13, (2020), pp.7-48.
19. Şenol, Dolunay, Erdem,Sezgin, Erdem, Elif, “IŞID: Küresel bir Terör Örgütü”, Fırat Üniversitesi Sosyal Bilimler Dergisi, 26 (2) (2016), pp. 277-292.
20. Veldhuis, Tinka, “Designing Rehabilitation and Reintegration Programs for Violent Extremist Offenders: A Realist Approach”, (ICCT Research Paper, March 2012).
21. UN General Assembly Resolution A/RES/70/291.

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.

"Scan to reach the software of this publication and the other products of COE-DAT"

www.coedat.nato.int