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.

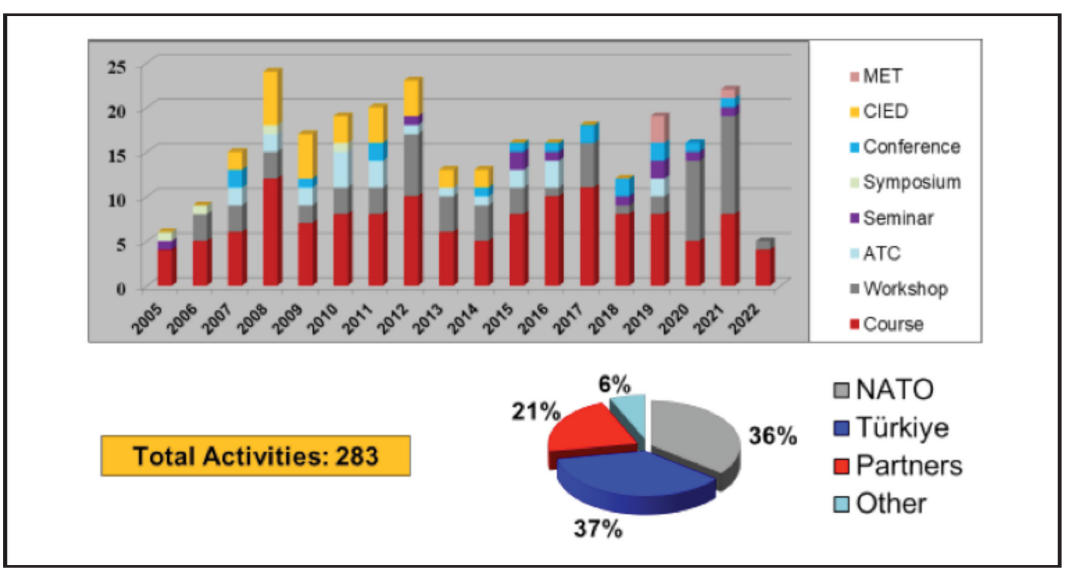

Figure 1. The Products of COE-DAT between 2005-2022.

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.

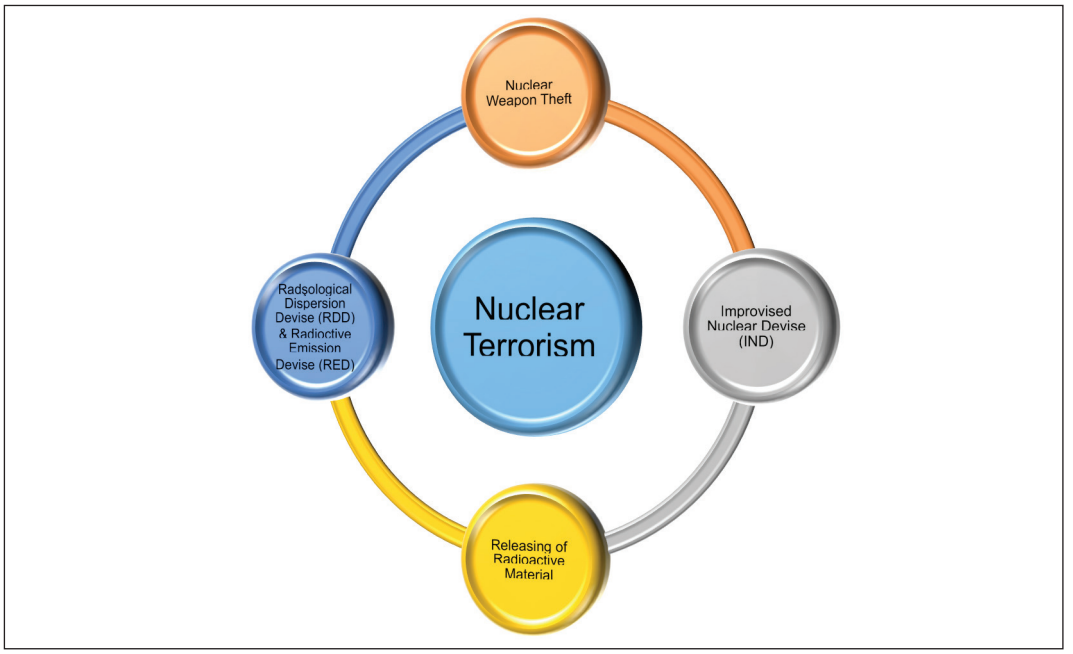

Figure 2. Four faces of nuclear terrorism for the securities (Jang et. al, 2021: 14)

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.

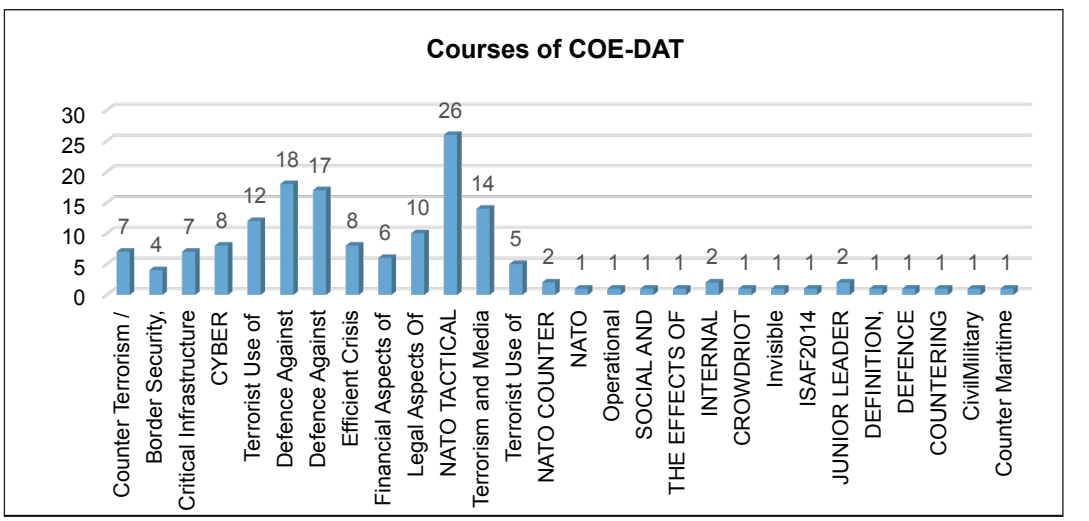

Figure 3. The courses of COE-DAT between 2005-2022.

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.

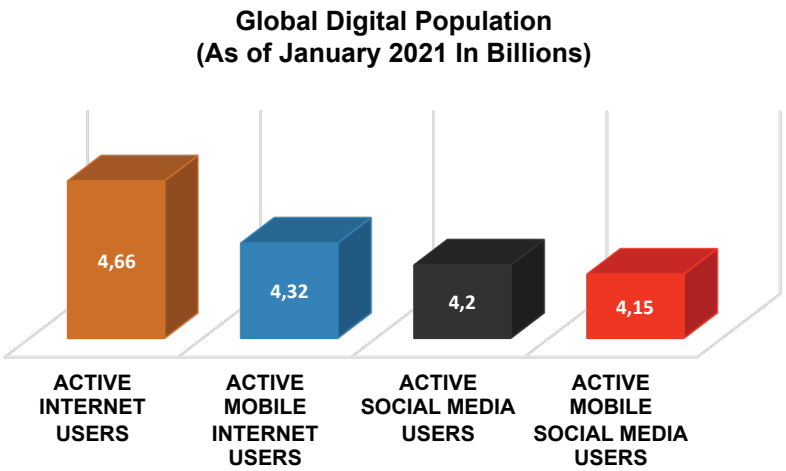

Figure 4. Global Digital Population (www.statista.com, Accessed April 22, 2022).

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/08WomenInTerrorism AndCounterterrorism.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.