Vol.2 • 2025

ISSN. 1307 - 9190

Defence Against Terrorism Review

DATR

Impact of the Cryptocurrencies and FinTech Innovations on Terrorist Financing Risks
Dr.Ivica SIMONOVSKI

Brand Archetypes and the Terrorist Organizations: The Case of Daesh
Dr.Ferit MALKARA - Dr.Çağatay BALCI

Beyond the Euro-Atlantic: Colombia's Path to NATO Global Partnership
Assoc.Prof.Dr.Başar BAYSAL

COE-DAT
Centre of Excellence Defence Against Terrorism

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

DATR is an international peer-reviewed journal

DATR is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT).

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

DATR dergisi uluslararası hakemli bir dergidir.

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

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

Yayın Sahibi: Halil Sıddık Ayhan
Sorumlu Yazı İşleri Müdürü: Ahmet Erol
Yayın Türü: Yerel Süreli Yayın
Yayın Şekli: Yıllık İngilizce

Defence Against Terrorism Review – DATR
Terörizmle Mücadele Mükemmeliyet Merkezi (TMMM)
Devlet Mahallesi İnönü Bulvarı
Süleyman Emin Caddesi No:65 06582
Çankaya/ANKARA
Tel: 0 (312) 425 8215
Faks: 0 (312) 425 6489
E-posta: datr@coedat.nato.int

Baskı: Başkent Klişe Matbaacılık
Bayındır Sokak No: 30/E
Kızılay/ANKARA
Basım Tarihi: Aralık 2025

Defence Against Terrorism Review
DATR

Vol. 2, 2025

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) is proud to present the 21nd Volume of its Defence Against Terrorism Review (DATR) journal. As in our previous issues, we have continued in this volume to publish well-researched articles with reliable information and practical recommendations. In doing so, we remain committed to the COE-DAT's mission to make contribution to the counter-terrorism efforts of NATO as well as its members and partner nations. Our current volume contains three insightful contributions to the literature exploring various aspects of terrorism and effective ways of countering terrorism.

The first article of this volume is entitled as "Impact of the Cryptocurrencies and FinTech Innovations on Terrorist Financing Risks". It is authored by Dr.Ivica Simonovski, who is the Co-Founder of Cyber Security Corporate Security and Crisis Management Initiative in North Macedonia. In his very interesting article, Dr.Ivica Simonovski explores the material risks involved in the terrorist uses of cryptocurrencies and FinTech innovations. The article conceive such risks as functions of three factors: threat, vulnerability, and consequence. Based on his analysis of the relationship between terrorism and cryptocurrencies as well as fintech innovations, Dr.Ivica Simonovski identifies the following trends: first, cryptocurrencies and FinTech innovations are being utilized by both terrorist organizations and lone actors for organizational and operational activities; second, there is a convergence of crime and terrorism financing; and lastly Non-Fungible Tokens (NFTs) are being created. Dr.Ivica Simonovski also notes that terrorist organizations and lone actors increasingly use online marketplaces in order to purchase weapons and ammunition. Dr.Ivica Simonovski recommends the development of global consensus on crypto regulation in order to fight against the terrorist uses of cryptocurrencies and FinTech innovations more effectively.

The second article, which is entitled as "Brand Archetypes and the Terrorist Organizations: The Case of DAESH", is authored by two independent researchers from Türkiye: Ferit Malkara and Çağatay Balcı. The article explores propaganda tactics of terrorist organizations by focusing on the case of DAESH. Among various terrorist propaganda tactics, the authors concentrate on the terrorist uses of brand archetypes for creating deeply resonant and symbolic representations of terrorist objectives. It is in this context that the article explores the propaganda tactics of DAESH as well as its strategy of disseminating its terrorist organizational brand globally. The article identifies that DAESH has employed several archetypes such as the "warrior" and the "savior" archetypes in order to make its terrorist propaganda. Based on its DAESH case study, the article concludes that terrorist groups use archetypes as psychological and symbolic tools in order to project greater influence for their terrorist agenda.

Last but not least, Dr.Başar Baysal from Ankara Bilim University in Türkiye also contributed to this issue with his insightful article entitled as “Beyond the Euro-Atlantic: Colombia’s Path to NATO Global Partnership”. The article explores Colombia’s experience in countering terrorism and other non-traditional security threats as well as the development of NATO’s relations with Colombia which is NATO’s first Latin American Global Partner. This author examines how the 2013 Security of Information Accord paved the way for Colombia’s elevation to a Global Partner status for NATO in 2018. The article notes that synergy in counter-terrorism training has fostered more robust intelligence-sharing channels and integrated responses to hybrid threats, including terrorism at domestic and international levels. The article demonstrates that Colombia as a post-conflict state has largely succeeded in relating NATO’s frameworks for modernizing its counter-terrorism policies. This article concludes that NATO’s flexible, interest-driven, and adaptive partnership with Colombia result in effective responses to global threats, including terrorism.

We wish to express our thanks to all authors and reviewers for their contributions to the current issue. We also hope that you may find the content of the current volume interesting and insightful. As always, we welcome receiving the invaluable insights and suggestions of our esteemed readers. We also invite new article submissions for our next issue. Please note that DATR is committed to welcoming and fostering contributions from both military and civilian backgrounds.

Sincerely yours,

Prof.Dr.Oktay F. Tanrısever
Editor-in-Chief

Defence Against Terrorism
Review DATR Magazine

DATR, 2025; 2 : 7-26
Electronic Online ISSN 1307 - 9190

Impact of the Cryptocurrencies and FinTech Innovations on Terrorist Financing Risks

Dr.Ivica Simonovski[1]

Abstract

With the rapid evolution of digital technology, terrorists are embracing cryptocurrencies and FinTech innovations. Some of the new financial services are not dependent upon or controlled by a bank or any central authorities that could govern their transactions. These new products and services have features such as speed, efficiency, and ease of use that benefit ordinary customers. These features also reduce the friction that terrorist financiers encounter when funding operations and organizations. This paper will expand the existing knowledge of competent counter-terrorism institutions about the risk posed by terrorists when using cryptocurrencies and FinTechFinTech for their organizational and operational needs.Risk can be seen as a function of three factors: threat, vulnerability, and consequence. When determining the risk, the following questions were considered:

(1) How do terrorists use technological advances to collect, move, store, and use funds to finance their organizational and operational activities, along with determining how to deal with the problem they have caused?

(2) To what extent are new financial technologies inclusive, and how are they regulated?

The information and views expressed in this article are solely those of the author's and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the author/s is affiliated.

1 Skopje, North Macedonia Financial Intelligence Office Head of CFT Department

(3) What are the capacities of government institutions and the financial sector to rapidly identify, track, and disrupt financial flows leading to terrorists?

The findings indicate that cryptocurrencies and FinTech innovations are being utilised by both terrorist organizations and lone actors for organizational and operational activities, the convergence of crime and terrorism financing, and the creation of Non-Fungible Tokens (NFTs). Furthermore, both terrorist organisations and lone actors used online retailers and marketplaces to purchase improvised explosive device components, weapons and ammunition to highlight their continued evolutions in the digital world. A global approach to crypto regulation would be ideal but has not yet been achieved. The likelihood that terrorists can exploit cryptocurrencies and FinTech innovations for their activities is therefore medium to high.

Keywords
Terrorists, terrorist financing, FinTech innovations, digital payments, cryptocurrencies.

1. Introduction

Emerging digital technology is driving changes not only in communication but also in the global financial system. FinTech innovations, products and services may offer significant economic opportunities. The primary purpose is to promote development and financial inclusion, enabling greater efficiency and speed in cross-border value transfer and improving safety for all customers. However, terrorists are technology-neutral and adaptive (Simonovski, I., & Unsal, Z., 2018).

In addition to traditional sources of funds, terrorists also need new sources of funds. Cryptocurrencies and FinTech innovations provide them with access to digital and crypto wallets, as well as an alphanumeric wallet address to send or receive digital or crypto assets to support their organizational and operational activities. Many online payment systems and cryptocurrencies are attractive to terrorist financiers as they enable them to conduct financial transactions anonymously or pseudo-anonymously, and peer-to-peer (P2P). Also, some of these platforms are poorly regulated and uncontrolled, especially when the payment system is under a relatively weak jurisdiction with serious strategic deficiencies to counter anti-money laundering/counter-terrorist financing/proliferation financing (hereafter: AML/CTF/PF) regime, which has been identified by the Financial Action Task Force (hereafter: FATF) (FATF-GAFI, 2024a).

In 2016, Europol was not able to confirm any reports of terrorist organizations using Bitcoin (EUROPOL, 2016). However, the first case where terrorists utilized crypto was in 2014, when a supporter of Daesh, who called himself 'Amreeki', provided guidelines on how to donate funds by using cryptocurrencies (Wile, 2014).

Digital currencies and cryptocurrencies have become the prominent currencies of the so-called Dark Web sites utilized by terrorists to purchase illicit goods such as weapons, explosives, ammunition, etc (Ward, 2018). However, the use of digital and cryptocurrencies and the Dark Web for terrorist activities has not been well-documented due to the lack of government capacity and some of the advantages these products offer, such as anonymity and speed. Although the evidence collected during investigations indicates that terrorists are already using both, more work is needed to ascertain how terrorists are using a combination of digital and cryptocurrencies and the Dark Web to finance both organizational and operational activities. This may be evidenced by the case with the Munich terrorist attacks in 2015, when German investigators concluded that a gunman, identified by an official as 18-year-old Ali David Sonboly, killed nine people in a shooting spree in Munich. Sonboly used a reactivated pistol he presumably purchased illegally on the so-called Dark Net (Bender, R., & Alessi, C., 2016).

Through case studies, this paper addresses the use of crypto transactions and FinTech innovations by terrorists in various parts of the world. At the same time, this paper also addresses the need for the unified regulation of cryptocurrency trading and FinTech innovations by individual countries. This will enable the timely identification of financial flows that lead to terrorist financing. Due to the underdeveloped capacities in various countries, terrorist financing investigations are limited and publicly available data cannot fully reflect the real picture of the level and frequency of the use of cryptocurrencies and FinTech innovations by terrorists.

Finally, this paper will provide recommendations for policy-makers that would contribute to more effective (security, political, social, and other) measures for addressing this threat more adequately and diminishing its consequences. This paper will also explore future challenges of terrorist financing issues, which should be among the top security priorities of NATO.

2. Why do Terrorist Actors Turn to Crypto and FinTech Innovations?

In today's globalized and multipolar world, terrorists are a key threat to in national, regional, and international security. Without having a strategy, it is challenging to defeat them. At the beginning of this paper, the focus will be on categorizing terrorists that use FinTech innovations, focusing on cryptocurrencies, crowdfunding platforms, online retailers and marketplaces, social media, and the Dark Web.

Terrorism as a form of action takes place in several stages, in which a range of activities that require funds are realized. Here, we come to one of the main motives for writing this paper: to explain the terrorist needs to increasingly exploit cryptocurrencies and FinTech innovations as a key element and driver for maintaining their organizational and operational activities. The funds are a prerequisite for the realization of organizational and operational activities and are often described as the 'fuel' or the 'bloodstream' of terrorists.

Terrorist groups are complex and vary in size, ideologies, operational reach, motivations, recruitment, tactics, behaviours, and capabilities. Despite differences among terrorist groups, the need for long-term and stable sources of funds to support the full range of operational and organizational activities they engage in is huge. Terrorists also vary widely in structure. In their research, Keatinge, Cerlisle, and Keen argue for several examples of a wide range of terrorists, including

"*lone actors, small cells and facilitation networks, command and control organizations, and territory-controlling groups"* (Keatinge, T., & Cerlisle, D., & Keen, F., 2018).

With the global emergence of Daesh, terrorism was enriched by another 'old-new phenomenon', the phenomenon of Foreign Terrorist Fighters" (FTFs) (Simonovski, I., & Unsal, Z., 2018). 'Old' because history speaks of foreign fighters, mercenaries, and volunteers, and 'new' because the term "FTFs" was first used and defined by the UN Security Council in 2014 (UNSCR, 2014). Drawing from these two approaches, this paper categorizes terrorists as follows:

a) **Members of Terrorist organizations:**
   - *Territory-controlling organizations* (such as Daesh, Boko Haram, or Al-Shabaab)
   - Command and control organizations without a single established headquarters (such as Al-Qaida)
b) **Members of Terrorist cells** – decentralized and independent small groups, inspired or connected to a terrorist organization.
c) **Foreign terrorist fighters** – individuals who are inspired by a terrorist organization and may have a formal or informal connection, and travel to conflict zones to engage in terrorist acts.
d) **Lone wolf** – individuals who may not have a formal connection to the terrorist organization, but who are generally inspired by it.

As a result of the strengthening of global efforts for countering terrorism financing, terrorists are increasingly looking to bypass their adversary's advantage by "abandoning the traditional modes of its financing" (Asif, H., & Nafees, S., &

Putz, C., 2022). Terrorist adoption of technology is an evolution, not a revolution, because these actors are adaptive and innovative in using cryptocurrencies and exploiting new FinTech innovations to finance their activities (Davis, 2021). A new generation of terrorist leaders and inspired members must be considered. They are increasingly IT tech-savvy engineers and a crop of dark 'visionaries' who view modern financial technology as a key operational gain that will give their group a 'first-mover advantage'.

3. Methodology

3.1. Purpose of the research

This paper aims to explore the extent to which cryptocurrencies and FinTech innovations pose new or exacerbate existing terrorist financing risks. Also, this paper should explore whether the risk of terrorist financing using cryptocurrencies and FinTech innovations has increased significantly over the past decade. Ultimately, however, the purpose of this paper is to point out to global and national stakeholders, including NATO members, allies and partners, that they can significantly mitigate the risks of terrorist financing by investing in modern blockchain analytics, harmonizing their regulatory approaches and implementing best investigative practices.

3.2. Research questions

Risk can be seen as a function of three factors: *threat, vulnerability, and consequence*.[2] When determining the risk, the following questions will be considered:

(1) How do terrorists use technological advances to collect, move, store, and use funds to finance their organizational and operational activities, along with determining how to deal with the problem they have caused?

(2) To what extent are new financial technologies inclusive, and how are they regulated?

(3) What are the capacities of government institutions and the financial sector to rapidly identify, track, and disrupt financial flows leading to terrorists?

---

[2] A **threat** is a person or group of people (terrorist actors), object, or activity with the potential to cause harm to, for example, the state, society, the economy, etc.. The concept of **vulnerabilities** as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. **Consequence** refers to the impact or harm that terrorism financing may cause and includes the effect of the underlying terrorist activity on financial systems and institutions, as well as the economy and society more generally. Read more: FATF Guideline: National Money Laundering and Terrorist Financing Risk Assessment, FATF-GAFI, February 2013, accessed on June 30, 2024, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html

3.3. Scope and limitation of the research

Limitations of this research design include restricted access to information held by the public sector on actual instances of terrorists or their supporters abusing cryptocurrencies and FinTech innovations for financing purposes. However, the key findings in this paper will be based on the publicly available investigated cases mentioned in this paper, in which terrorists have used cryptocurrencies and FinTech innovations.

3.4. Data gathering and analysis

Whether and how terrorists would use cryptocurrencies and FinTech innovations depends on the available technology and its properties, as well as the groups' needs and capabilities. Analysis shows that newer payment systems and cryptocurrencies have emerged with properties that terrorists find more anonymous and attractive than those previously available. For example, if another cryptocurrency provides better anonymity than Bitcoin for large-sum transactions and is more widely adopted than Monero, Zcash, Dash, and Verge, then terrorists might be inclined to exploit that currency for its organizational and operational activities. When French authorities arrested 29 Daesh and al-Qaeda supporters in September 2020 for organizing financial support, Daesh reportedly moved to accept Monero (XRM) (France24, 2020). Considering these nuances, to assess the impact of FinTech innovations on terrorist financing risk, it is important to look at various terrorist groups to analyse who they are and how they exploit technology advancements such as digital payments, cryptocurrency and the Dark Web as an alternative to traditional sources to raise, move and use funds to finance their organizational and operational activities.

Social media platforms such as Facebook, Instagram, TikTok, and YouTube have become a field for spreading radical ideology, recruiting new members, and launching donation campaigns (Weimann, G., & Pack, A., & Sulciner, R., & Scheinin, J., & Rapaport, G., & Diaz, D., 2024). When Twitter, Facebook, and YouTube crack down on extremist propaganda, Daesh recruiters are exploiting lesser-known encrypted messenger apps designed for businesses and gamers, such as RocketChat, Yahoo Together, Viber, Discord, Telegram, and TamTam to enable them to curate, tailor, upload, and disseminate content more effectively from their phones or computers (Katz, 2019).

3.4.1. Using Cryptocurrencies and FinTech Innovations for Funding Organizational and Operational Activities

For organizational funding, social media, encrypted lesser-known messenger apps (such as Twitter and Telegram), crowdfunding platforms, and cryptocurrencies (such as Bitcoin and Monero) have been highlighted as tools for raising and moving funds. Some of the world's richest terrorist organizations use crypto funding infrastructure to raise and move funds.

In 2014, Daesh lost most of the territory it controlled in Iraq and Syria (Popper, 2019). A pro-Daesh blog, 'Al-Khilafah Aridat: The Caliphate Has Returned' has provided instructions to Daesh members and supporters on how Bitcoins could subsequently be used to fund the caliphate. This was one of the reasons for shifting to online and virtual fundraising (Charles, 2014). Another example is Ali Shukri Amin, a 17-year-old U.S. resident who used his own Twitter account, '@ Amreekiwitness', to provide support and guidelines to Daesh and its supporters by teaching them how to use Bitcoin and how to hide it using an encryption platform (Abutaleb, Y., & Cooke, K., 2016).

In the beginning, terrorist organizations faced some challenges with how to turn Bitcoin and other cryptocurrencies into fiat currencies in the territory it controlled. Many of those territories, such as Iraq and Syria, Africa, and some parts of Asia, do not have the technology to convert large amounts of Bitcoin into fiat currencies. However, some countries with developed financial systems have been used by terrorist organization members and supporters to convert crypto assets into fiat currencies through Bitcoin ATMs and vice versa. Terrorist organizations have used assets to maintain organizational activities such as recruitment, online propaganda, etc.

For operational funding, cryptocurrencies, payment service providers such as Payoneer and PayPal, online retailers and marketplaces like eBay, Amazon, and Dark Net Platforms, as well as social media, have been utilised in several cases. But in the case of lone actors, the financial resources needed to commit an attack are often quite low. In January 2016, IT expert Bahrun Naim, one of the most notorious militants and Daesh fighters in Indonesia, used online payment services such as PayPal and Bitcoin to transfer money to the PayPal accounts of the wife of Arif Hidayatullah and Nur Rohman, two fellow Daesh militants, who used the funds to finance several suicide bombings in Jalan Thamrin in Jakarta. (Soeriaatmadja, 2017). Stephan Balliet, a German far-right gunman behind the Halle synagogue shooting, received 0.1 Bitcoin from an anonymous online donor before the attack. He used Bitcoin to purchase components for his handmade weapons (Caniglia, M., & Winkler, L., & Metias, S., 2024).

In general, two main typologies can be identified.

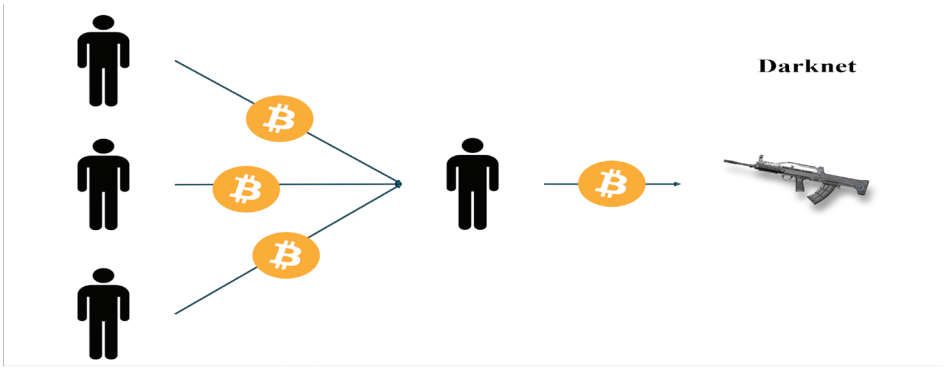


Figure 1: A lone actor received Bitcoins and used them on the Dark Net to purchase a weapon.

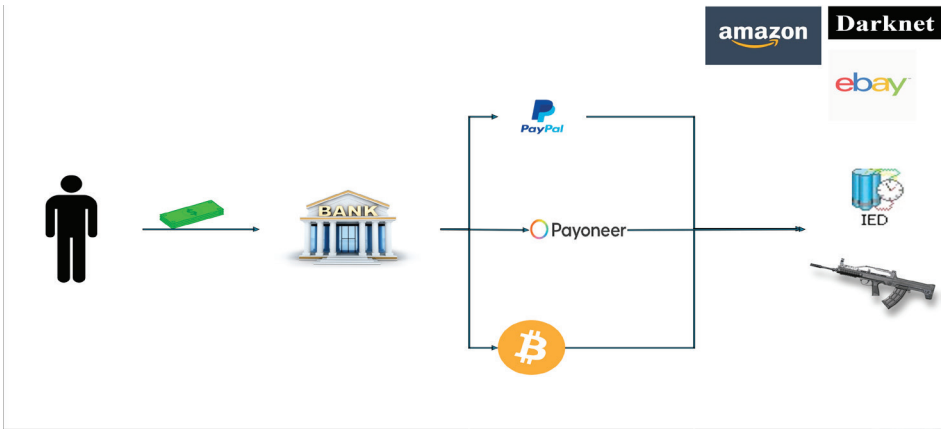


Figure 2: A lone actor uses his own money to purchase IED components and weapons via online retailers and the Dark Net utilizing an online payment system and Bitcoin.

Considering the relatively small number of cases with explicit evidence of the use of cryptocurrencies and FinTech innovations for operational activities by terrorist organizations, there are a few cases in which terrorist organizations have used them. According to identified typologies, many of the cryptocurrencies were used to purchase weapons, ammunition and components for Improvised Explosive Devices (IEDs) through online stores, marketplaces, and the Dark Web. In another single case, 28-year-old Hisham Chaudhary converted tens of thousands of British pounds to Bitcoin to fund the extraction of Daesh supporters from detention camps and smuggle them back into Daesh-controlled territory (BBC, 2021).

3.4.2. Other Potential Risks

3.4.2.1. The Convergence of Crime and Terrorism Financing

The analysis detected and identified several hybrid crime typologies involving the combination of loan fraud and fraudulently obtained debit and credit cards to purchase cryptocurrencies, profiting from crypto Ponzi schemes and extortion in Bitcoin by lone actors. In 2017, a lab technician, Zoobia Shahnaz, a 27-year-old resident of Long Island, was involved in a fraudulent scheme targeting several financial institutions to obtain money for Daesh. The illicit money received was used to buy Bitcoin and other cryptocurrencies and to make transfers to various Daesh sympathizers as well as companies abroad (US DoJ, 2020). In another example, Leopard Wisnu, a 29-year-old Indian IT worker, who was inspired by Daesh and motivated by extortion, decided to threaten the Alam Sutera Mall with a bomb and demanded to be paid 100 Bitcoins. When management responded by sending him 100 Bitcoins, he activated the bomb in the mall's toilet, injuring one individual (The Jakarta Post, 2015).

3.4.2.2. The Creation of Non-Fungible Tokens and Other Advanced Uses

Creating products from which a material benefit can arise is also a risk. In practice, terrorists look to utilise more advanced and innovative applications to create their products to gain financial benefit. In 2022, a Daesh supporter created a **Non-Fungible Token** to raise money and to praise militant groups for an attack on a Taliban position in Afghanistan (Talley, 2022). When they are purchased through a digital marketplace and transacted with an anonymous wallet, this could essentially result in an untraceable transaction, making them vulnerable to exploitation by terrorists. This is potentially a red flag, considering terrorists can embrace blockchain technology to avoid sanctions and generate funds for their operational and organizational costs.

The creativity of terrorists and their supporters was highlighted through the sale of **Cryptocurrency Coupons**. In 2020, 29 supporters linked to al-Qaeda organized a cryptocurrency-based terrorism financing scheme to sell cryptocurrency coupons to support organizational activities. The coupons were credited to various accounts opened abroad by members of al-Qaeda and Daesh, who then converted them into Bitcoin (Chainanalysis, 2021).

Then, in 2019, Brenton Tarrant, a New Zealand shooter, profited from a notorious **Crypto Pyramid Scheme**. He invested his money in a cryptocurrency called BitConnect, which experts said was an infamous pyramid scheme (DeSilva, 2019).

4. Cryptocurrencies and FinTech Ecosystem, Financial Inclusion and Regulation

The concept of vulnerabilities, as used in a risk assessment, comprises those things that could be exploited by the threats (in this paper, terrorist groups) or that may support or facilitate their activities. A lack of understanding of cryptocurrencies and the FinTech ecosystem will result in ineffective policies in combating terrorist financing. This paper will now, therefore, focus on cryptocurrencies and FinTech products that can be used or misused by terrorists.

FinTech ecosystems are oriented towards developing and adopting new technologies and helping users better manage their financial operations, processes, and lives. It consists of specialized software and algorithms installed on IT devices such as smartphones, tablets, and computers.

4.1. Crypto Ecosystem

This section defines key terms and technologies in the crypto ecosystem.

Cryptocurrencies are decentralized virtual digital money, allowing individuals, including terrorists, to transfer funds anonymously. However, a cybersecurity expert mentioned six closely linked features of these currencies that limit their use. These are "*anonymity, usability, security, acceptance, reliability, and volume"* (Vujic, 2025). For instance, the volume of crypto transactions would increase if the cryptocurrencies were accepted in more places and were more reliable for consumers. The anonymity depends on the following factors, both technical and operational:

Technical factors	Operational factors
Owned by a cryptographic private key, not by people or institutions.	Single public/private key pair
Coin mixer to hide ownership and obscure the origin and destination.	"The Onion Router" **TOR** network or "Invisible Internet Project" **I2P** and stealth address to hide IP address

***Table 1**: Technical and Operational Factors* (Vujic, 2025)

Stablecoins are a subset of cryptocurrency whose value is pegged to traditional assets, typically government-issued fiat currencies such as the U.S. dollar or gold to maintain a stable price. Terrorists can exploit stablecoins to layer in money laundering schemes to convert fiat to cryptocurrency or vice versa, and properly use them (FATF-GAFI, 2020). Although no data has yet been recorded on the use of stablecoins by terrorists, we emphasise the risk of when and how terrorists can use them.

Terrorists can also use **Crypto Automated Teller Machines (Crypto ATMs)** to convert cash for cryptocurrency or vice versa. According to Coinatmradar statistics, **38156 Crypto ATMs** in total have been registered in **70 countries** (Coinatmradar, 2024). Jacob Wade addresses the limitations of using crypto ATMs, such as high fees, transaction limits, availability, and security (Wide, 2024). However, they might be used as a tool for terrorists to evade Anti-Money Laundering/Counter Terrorist Financing standards and convert cash to crypto or vice versa by using fake documents when creating virtual wallets.

Unhosted Wallets allow users to install personal wallets on their mobile phones or other devices to store their crypto, which might be fully offline. Financial Action Task Force's guidance considers transactions with unhosted wallets as a potentially higher risk and provides Virtual Assets Service Providers (VASPs) with options to treat them as such (FATF-GAFI, 2024b). Unhosted wallets can serve as a vehicle for terrorists to move funds between regulated exchanges.

Peer-to-Peer Transactions are transfers between two unhosted wallets without a third party in Decentralized Finance (DeFi). In this process, users are acting on their own behalf. Potentially, terrorists can use peer-to-peer transactions to move untraceable funds to avoid AML/CTF controls (Know Your Customer (KYC) and Customer Due Diligence (CDD)). Also, terrorists might use funds from unhosted wallets to procure weapons and IED components directly on the Dark Net, avoiding detection by investigators.

Decentralized Exchanges play an essential role in the crypto ecosystem. The anonymity and lack of regulation of the decentralized exchanges enable terrorist actors to easily convert their fiat currencies into cryptocurrencies or vice versa, or crypto to crypto, making it difficult for authorities to track and seize the funds. Some exchanges do not apply KYC procedures to verify a customer's identity (Nallapaneni, 2024).

Cryptocurrency mixers, which might be *centralized custodial mixers*[3] and *non-custodial mixers.*[4] Both mixers can be useful techniques for terrorists to obfuscate the origins and owners of the funds because these services blend multiple crypto transactions and make legal transactions anonymous. For the experts, terrorists can use non-custodial mixers for financial privacy and money laundering schemes.

Non-Fungible Tokens (NFTs) can also be used by terrorists for fundraising (Gluck, R., & Binder, L., 2023). We have already explained how Daesh supporters created a **Non-Fungible Token** to raise money and to praise militant groups for an attack on a Taliban position in Afghanistan.

---

[3] ***Centralized custodial mixers*** temporarily take ownership of the user's funds and are run by a single operator

[4] ***Non-custodial mixers*** are built into privacy wallets and smart contracts mixers that do not blend users' funds in just one transaction.

4.2. Internet-Based Payment Systems (IBPS)

Internet-Based Payment Systems (IBPS) have become an integral part of modern financial transactions as they are fully interconnected with traditional financial payment systems. For instance, funds can be moved easily from the bank account to these platforms. These IBPSs have started to issue prepaid cards to their clients, granting them access to worldwide ATM networks. Besides that, IBPS allows individuals to send money digitally in the shortest period, enable shopping, and conduct peer-to-peer transfers via mobile payment applications such as Venmo, Cash App, PayPal, Payoneer, etc. Also, individuals can store funds on mobile wallets such as Google Pay, Apple Pay, PayPal, Payoneer, etc (Tsymbaliuk, 2024). These payment systems can also allow for non-face-to-face business relationships, which may exacerbate the risks of identifying fraud or the purposeful use of inaccurate information to conceal illicit activities.

IBPSs such as PayPal, Payoneer, Payer, etc., have been used by terrorists to transfer electronic money or value to other individuals who also hold accounts with the same provider, as well as to purchase equipment, clothing, knives and IED components. Some of the aforementioned cases, indicates that lone actors used IBPS in the operational phase.

4.3. Dark Web

The Dark Web is the part of the World Wide Web that is hidden from plain view and requires special software to access, enabling users to gain anonymity and make tracking difficult. Terrorists are increasingly exploiting the Dark Web to raise funds through crypto donations, extortion, and even organized crime activities against the population, such as human and organ trafficking. Traditional search engines such as Firefox, Google, and Mozilla do not index the Dark Web's content. To gain access to the Dark Web, terrorists use special software such as The Onion Router or Invisible Internet Project. Blocking traffic to websites at specific choke points along the internet hierarchy does not work with encrypted overlay networks. This advantage allows the Dark Web to be more resistant to surveillance by governments and regulators (Kumar, 2024). In an isolated case in October 2023, a Daesh supporter sold gift cards on the Dark Web for less than face value to support Daesh (U.S. Department Of Treasury, 2024). In another case, the terrorist organization Islamic State Khorasan Province, through its magazine Voice of Khorasan, asked followers and sympathizers to make donations in cryptocurrencies like Monero (XMR) via the Dark Web (OpIndia, 2023).

4.4. Online Retailers and Marketplaces

Terrorists can use Online Retailers and Marketplaces such as eBay, Amazon, or Alibaba to procure weapons, ammunition, IED components, and other goods and materials via bank or internet payment systems such as PayPal for their organizational and operational activities. They have also used these platforms to sell goods and raise funds to support their activities. Case analysis showed that lone actors primarily use these platforms when conducting operational activities to procure weapons or IED components. A good example is Mohammed Rehman, the London Underground attacker, who bought chemical precursors and other materials on eBay by using a PayPal account (Bowcott, O., 2023).

4.5. Social Media, Encrypted Messaging, and Crowdfunding Platforms

Crowdfunding is a process where a 'crowd' raises funds by collecting small amounts of money from donors, often via the Internet. Solicitation of donations, often under the guise of charitable activity through social media channels and crowdfunding platforms, is one of the most common forms of crypto-based terrorist financing. Terrorists have outreach to a large audience through peer-to-peer horizontal communication such as chats and forums, social networks (Facebook, Twitter, Instagram), and mobile applications (WhatsApp, Viber).

FATF recognized that some social media sites and messaging apps can offer encrypted messaging services to secure conversations and documents (FATF-GAFI, 2023a). Terrorists can use this to share financial data, campaign information, and donation instructions to their networks.

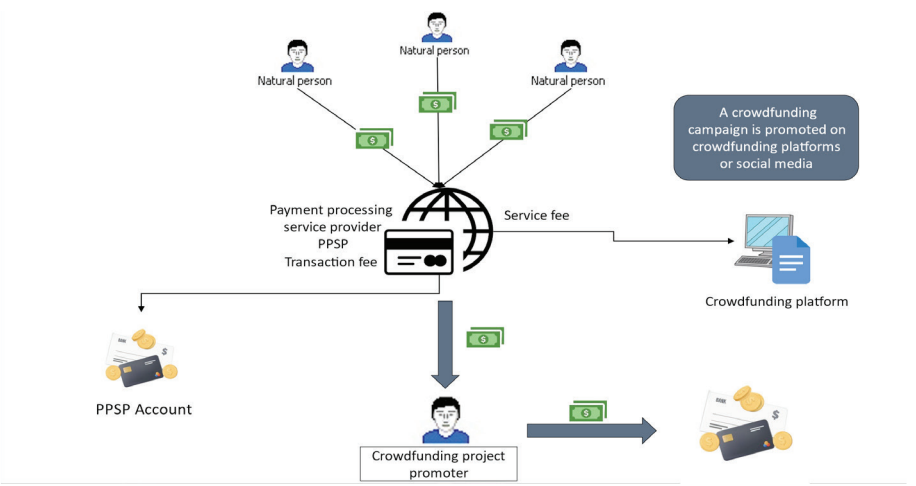


Figure 3: Crowdfunding donation campaign scheme

A good example is Hajjaj Bin Fahd al Ajmi, a Kuwaiti national, designated by the United Nations Security Council as a supporter of a terrorist organization. He was engaged by Al-Nusrah Front to organize a Twitter fundraising campaign (Counterextremism, 2024). Experts argued that transactions can occur instantaneously and anonymously by combining social media, financial technologies, and cryptocurrencies. Often, terrorists use charities to bypass platform policies.

4.6. Cryptocurrencies and Financial Inclusion: Too Risky to Embrace, Too Compelling to Ignore

What is the best approach to regulating something borderless in its nature, open-source, decentralized and constantly evolving? Cybersecurity experts argue that cryptocurrencies are too risky to embrace and too compelling to ignore.

The risk of using crypto assets and financial technologies by terrorists directly depends on internet coverage. In April 2024, there were 5.44 billion internet users worldwide, which amounted to 67.1 per cent of the global population (Kemp, 2024). Internet availability, the wide range of cryptocurrencies, and new and emerging challenges linked to technological innovation in the ecosystem increase the risk of their use by terrorists (European Commission, 2021). As an illustration, the risk is low in the Maghreb area, where terrorists use traditional means of financing such as Hawala, compared to those operating in countries with high internet access. For illustration, the Hawala system does not meet AML/CTF standards such as KYC and CDD.

The FATF standards require countries to assess and mitigate the risk associated with Virtual Asset Service Providers (VASPs) and activities, to regulate the license and registration process, and to supervise them through competent national authorities, such as the National Bank, the Financial Intelligence Unit, etc (FATF-GAFI, 2021b). With this, the countries must regulate all types of VASPs, such as fiat currency to crypto and vice versa, custodian wallets, and crypto-to-crypto exchanges. As obliged AML/CFT entities, VASPs are required to provide KYC and CDD procedures, collect information about transaction parties, and reduce levels of anonymity (FATF-GAFI, 2021a). However, countries around the world do not speak with one voice regarding crypto regulation. A global approach to crypto-asset regulation would be ideal, but there are a few challenges in achieving this goal that directly have an impact on regulation, such as:

- Different classifications and understandings.
- Lack of standardized definitions.
- Absence of the ability to seek regulatory arbitrage as a consequence of varying jurisdictional oversight.

- Lack of human and IT capacities.
- National, regional, and global monitoring, supervision, and enforcement.

FATF Recommendation 15 requires IBPSs to be subject to AML/CFT regulation and supervision, and to provide KYC and CDD procedures (FATF-GAFI, 2021b).

Donation-based crowdfunding platforms connect donors with fundraisers. In general, FATF does not recognize crowdfunding platforms under the definition of financial institutions (Thomson Reuters, 2022). They cooperate with their partners through payment processors or money value transfer systems defined as financial institutions. Based on the FATF questionnaire, not all countries have regulated crowdfunding platforms within the scope of their AML/CFT regimes (FATF-GAFI, 2023b).

Lacking a global umbrella organization, the European Union (EU) requires hosting service providers (HSPs) to identify and remove terrorist-related content, which includes fundraising campaigns, from their platforms (EU-Monitor, 2021). Although the regulation does not specify whether service providers should remove fundraising campaigns, this question for experts is the basis for further cooperation and building a public-private partnership between investigative authorities and service providers, which would enable the introduction of internal procedures for recognizing suspicious donation campaigns intended for terrorist purposes.

5. Conclusion and Recommendations

Financial exclusion from traditional financial networks and systems has led the new generation of terrorists and their leaders to exploit cryptocurrencies and FinTech innovations to support their organizational and operational needs.

The limited availability of data sets and evidence remains the biggest issue in comprehensively assessing the impact of FinTech innovations on terrorist financing risk. This reflects the weak technical and human capacities of financial and government institutions to collect evidence. Therefore, the key findings in this paper are based on numerous publicly available investigated cases.

This paper addressed the three research questions posed in the introduction.

The terrorist threat has been assessed as medium to high. The terrorist organizations and lone actors that exploit cryptocurrencies and FinTech innovations have been unmasked, and their activities decrypted.

In general, cryptocurrencies and FinTech innovations are being used by both terrorist organizations and lone actors for:

a) Organizational and operational activities,

b) The Convergence of crime and terrorism financing

c) Creation of Non-Fungible Tokens (NFTs) and other advanced uses.

Furthermore, both terrorist organizations and lone actors used online retailers and marketplaces to purchase IED components, weapons and ammunition to highlight their continued evolutions in the digital world.

The risk is not generalized to all cryptocurrencies and FinTech innovations and is greater in some sectors than in others. However, analysis indicates that the risk can be exacerbated when terrorists use cryptocurrencies and FinTech innovations in tandem with traditional financial methods.

A global approach to crypto regulation would be the ideal, but this has not yet been achieved. In some jurisdictions, decentralized exchanges do not meet the AML/CTF criteria. Other areas, such as social media, online retailers, marketplaces and the Dark Net, do not have AML/CTF obligations and continue to operate separately. The likelihood that terrorists can exploit cryptocurrencies and FinTech innovations for their activities remains medium to high.

Cryptocurrencies and FinTech Innovations that enable a high volume of funds to be raised, moved, or used for Terrorist Financing purposes have higher consequences. The consequences for many Terrorist Financing risks are likely to be more severe, which impacts how jurisdictions should respond to identified threats and dedicate the appropriate resources to dedicate to combating identified risks and the types of mitigating measures to put into place.

By evaluating *threats, vulnerabilities, and consequences,* the impact of new technology on terrorism financing risk is **medium to high**.

Because there is no single silver bullet to defeat these threats, this paper recommends a multi-stakeholder and comprehensive risk-based approach that encourages countries to continuously monitor how terrorists raise, move, and use funds, such as:

- **Rec 1**: Before taking any action, the countries should identify, assess and understand the Terrorist Financing risk for their respective country and take action to ensure that the risk is mitigated effectively. The key findings of the assessment should be fact-based.
- **Rec 2**: The countries should assess the nature, size and risk associated with all types and methods of cryptocurrencies and FinTech innovation and consider how those may be changing over time.
- **Rec 3:** The countries should apply a risk-based approach to mitigate Terrorist Financing and ensure that:

- Public institutions, regulators, and financial institutions should ensure that their laws, internal policies, standard operating procedures, and transaction monitoring systems are adequately considering Terrorist Financing.
- Full implementation of FATF Recommendation 15 on Virtual Assets and Virtual Assets Service Providers regulation.
- Social media, crowdfunding platforms, online retailers and marketplaces, and the Dark Net should have a legal responsibility to identify and properly report suspicious terrorist financing information to public institutions.
- Applying a multi-stakeholder approach and creating a public-private 'FinTech - Crypto Alliance' partnership, composed of the public and private sector (financial institutions, FinTech, and Crypto companies). This approach is useful because public institutions will never have as much FinTech expertise as the private sector.

In conclusion, terrorist finance risk assessment is an ongoing process. In that regard, all key findings and the overall conclusion made by this research are provisional and will need to be addressed again in the years to come.

References

Abutaleb, Y., & Cooke, K. (2016, June 6). *Reuters*. Retrieved from Extremists Among Us: A teen's turn to radicalism and the U.S. safety net that failed to stop it: https://www.reuters.com/investigates/special report/usa-extremists-teen/

Asif, H., & Nafees, S., & Putz, C. (2022, February 04). *The Diplomat.* Retrieved from Cryptocurrency and Terrorist Financing in Asia: https://thediplomat.com/2022/02/cryptocurrency-and-terrorist-financing in-asia/

BBC. (2021, September 3). *BBC.* Retrieved from Oadby Terrorist Who Funded IS with Bitcoin Jailed: https://www.bbc.com/news/uk-england-leicestershire-58439085

Bender, R., & Alessi, C. (2016, 24 July). *The Wall Street Journal.* Retrieved from Munich Shooter Likepy Bought Reactivated Pistol on Dark Net: https://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686

Bowcott, O. (2023, October 6). *The Guardian News*. Retrieved from ISIS Mouthpiece Calls for Donations in Monero (XMR): https://www.theguardian.com/uk-news/2015/dec/29/couple-guilty-july-7-anniversary-bomb-plot-london

Caniglia, M., & Winkler, L., & Metias, S. (2024, June 30). *European Strategic Intelligence and Security Center.* Retrieved from The Rise of the Right - Wing Violent Extremism Threat in Germany and its Transnational Character: http://www.esisc.org/upload/publications/analyses/the-rise-of-the-right-wing-violent-extremism-threat-in-germany-and-its-transnational-character/The%20Rise%20of%20the%20Right-Wing%20Violent%20Extremism%20Threat%20in%20Germany%20and%20its%20Transnational%2

Chainanalysis. (2021, February 01). Retrieved from The 2021 Crypto Crime Report: https://go.chainalysis.com/2021-Crypto-Crime-Report-demo. html?aliId=eyJpIjoiczZxaHRDT3M1Nno0TkgrWiIsInQiOiI1STdPOUZ4bnJNXC9mNksxOW1oc0Z1UT09In0%253D

Chainanalysis. (2022). *The 2022 Crypto Crime Report.* Chainanalysis.

Chainanalysis. (2024, March 26). *Chainanalysis*. Retrieved from Israeli Authorities Disrupt Hezbollah and Iran Quds Force Terrorism Financing Crypto Infrastructure Seize $1.7 Million in First: https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/

Charles, B. S. (2014, October 29). *Security Intelligence* . Retrieved from ISIS. Are They Using Bitcoins to Fund Criminal Activities: https://securityintelligence.com/isis-are-they-using-bitcoins-to-fund-criminal-activities/

Coinatmradar. (2024, July 03). *Coinatmradar*. Retrieved from Bitcoin ATM Map: https://coinatmradar.com/

Counterextremism. (2024). *Counter Extremism Project*. Retrieved from Hajjaj Bin Fahd Al Ajmi: https://www.counterextremism.com/extremists/hajjaj-bin-fahd-al-ajmi

Davis, J. (2021, July 19). *Global Network of Extremism and Technology.* Retrieved from Technology and Terrorist Financing: https://gnet-research.org/2021/07/19/technology-and-terrorist-financing/

DeSilva, M. (2019, March 19). *Quartz*. Retrieved from The New Zeland shooter profited from a notorius crypto pyramid scheme: https://qz.com/1575323/the-new-zealand-shooter-got-rich-off-crypto-scam-bitconnect

EU-Monitor. (2021, December). *EU-Monitor.* Retrieved from Regulation2021/784-Addressing the Dissemination of Terrorist Content Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784

European Commission. (2021, July 20). *European Commission.* Retrieved from Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690

EUROPOL. (2016, July 2020). *EUROPOL.* Retrieved from EU Terrorism Situation and Trend Re-

port: https://www.europol.europa.eu/publications-events/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016

Fanusie, Y. (2016, August 24). *The Ciper Brief*. Retrieved from The New Frontier in Terror Fundraising: Bitcoin: https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin#:~:text=The%20Ibn%20Taymiyya%20Media%20Center%20%28ITMC%29%2C%20an%20online,verifiable%20instance%20of%20a%20terrorist%20group%20using%20bitcoin.

FATF-GAFI. (2020, June 01). *FATF.* Retrieved from FATF Report to the G20 Finance Ministers and Central Bank Governors on so-colled Stablecoins: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf

FATF-GAFI. (2021a, October 01). *FATF.* Retrieved from Virtual Assets and Virtual Assets Service providers: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

FATF-GAFI. (2021b, October 01). *FATF Guidelince.* Retrieved from Virtual Assets and Virtual Assets Service Providers - Updated Guidence for a Risk-Based Approach: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

FATF-GAFI. (2023a, October 01). *FATF.* Retrieved from Crowdfunding for Terrorism Financing: https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html

FATF-GAFI. (2023b, November). *FATF Recommendations.* Retrieved from FATF Recommendations: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

FATF-GAFI. (2024a, June 25). *Financial Action Task Force.* Retrieved from Black and Grey List: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

FATF-GAFI. (2024b, July 02). *FATF.* Retrieved from Virtual Assets and Virtual Assets Service Providers - Updated Guidance for a Risk - Based Approach: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

France24. (2020, September 29). *France 24*. Retrieved from France srrests 29 in anti - terror Syria financing sting: https://www.france24.com/en/20200929-france-arrests-29-in-anti-terror-syria-financing-sting

Gluck, R., & Binder, L. (2023, July 10). *Global Network on Extremism & Technology*. Retrieved from Are Jihadists Profiting from NFTs?: https://gnet-research.org/2023/07/10/are-jihadists-profiting-from-nfts/

Katz, R. (2019, January 9). *Wired*. Retrieved from A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps: https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/

Keatinge, T., & Cerlisle, D., & Keen, F. (2018, May 27). *European Parliament's Special Committee on Terrorism.* Retrieved from Virtual Currencies and terrorist financing: assessing the risk and evaluating responses: http://www.europarl.europa.eu/supporting-analyses

Kemp, S. (2024, April 24). *Digital 2024 April Global Statshot Report.* Retrieved from DATAREPORTAL: https://datareportal.com/reports/digital-2024-april-global-statshot

Kumar, V. (2024, July 02). *Vikaskumar91490*. Retrieved from Advantages and Disadvantages of the Dark Web: https://vikaskumar91490.medium.com/advantages-and-disadvantages-of-the-dark-web-c834462bca48

Nallapaneni, D. (2024, March 01). *CoinLedger*. Retrieved from 14 Non-KYC Exchangers: https://coinledger.io/blog/non-kyc-exchanges

OpIndia. (2023, October 06). *Opindia*. Retrieved from ISIS Mouthpiece Calls for Donations in Monero (XMR): https://www.opindia.com/2023/10/isis-magazine-jihad-monero-terrorist-activities-cryptocurrenc-india-nirmala-sitharaman/

Popper, N. (2019, August 18). *NYTimes*. Retrieved from Terrorist Turn to Bitcoin for Funding, and They're Learning Fast: https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html

Reuters, T. (2024, July 05). *thomsonreuters.com.* Retrieved from Cryptocurrencies regulation by country: https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf

Simonovski, I., & Unsal, Z. (2018). *Countering the Financing of Terrorism in the International Community.* Berlin: Peter Lang GmbH.

Soeriaatmadja, W. (2017, January 14). *The Straits Times.* Retrieved from Millitant Bahrun Naim used PayPal Bitcoin to Transfer Funds for Terror Attack in Indonesia: https://www.straitstimes.com/asia/se-asia/militant-bahrun-naim-used-paypal-bitcoin-to-transfer-funds-for-terror-attacks-in

Talley, I. (2022, September 5). *Biznews*. Retrieved from Bad News for Crypto - ISIS explores NFTs for funding: https://www.biznews.com/global-citizen/2022/09/05/crypto-isis-nft-funding

The Jakarta Post. (2015, October 30). *The Jakarta Post.* Retrieved from Alam Sutera bomber says he was trying to reply debts: https://www.thejakartapost.com/news/2015/10/30/alam-sutera-bomber-says-he-was-trying-repay-debts.html

Thomson Reuters. (2022). *Thomson Reuters.* Retrieved from Cryptocurrencies regulation by Country: https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf

Tsymbaliuk, I. (2024, June 18). *Rates*. Retrieved from Digital Payment Services in 2024: Key Trends and Payment Methods: https://rates.fm/payment-systems/exploring-global-online-payment-systems-key-trends-in-2023/

U.S. Department Of Treasury. (2024). *2024 National Terrorist Financing Risk Assessment.* Washington: US department of Treasury.

UNSCR. (2014, September 24). *United Nation.* Retrieved from UN Security Counciul Resolution 2178, S/RES/2178: https://documents.un.org/doc/undoc/gen/n14/547/98/pdf/n1454798.pdf?token=qPZlzbOoMzUtFCX4IO&fe=true

US DoJ. (2020, February 7). *US Department of Justice.* Retrieved from Case: United States vs. Zoobia Shahnaz: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Zoobia%20Shahnaz%20Govt%20Sentencing%20Letter.pdf.

Vujic, A. (2025, July 02). Cryptocurrencies characteristics. (I. Simonovski, Interviewer)

Ward, A. (2018, January 22). *RAND.* Retrieved from Bitcoin and the Dark Web: The New Terrorist Threat?: https://www.rand.org/pubs/commentary/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html

Weimann, G., & Pack, A., & Sulciner, R., & Scheinin, J., & Rapaport, G., & Diaz, D. (2024). Generating Terror: The Risk of Generative AI Exploatation. *Combating Terrorism Center Volume 19 Issue 1*, 17-25.

Wide, J. (2024, March 10). *Investopedia*. Retrieved from What is a Crypto ATM?: https://www.investopedia.com/crypto-atm-6456118#:~:text=Crypto%20ATMs%20are%20kiosks%20that,%E2%80%9CBitcoin%20ATM%20Map.%E2%80%9D

Wile, R. (2014, July 8). *Business Insider*. Retrieved from Supporter of Extremist Group ISIS Explain How Bitcoin Could BE Used To Fund Jihad: https://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7

Defence Against Terrorism
Review DATR Magazine

DATR, 2025; 2 : 7-26
Electronic Online ISSN 1307 - 9190

Brand Archetypes and the Terrorist Organizations: The Case of Daesh

Dr.Ferit Malkara[1]*- Dr.Çağatay Balcı*[2]

Abstract

In the recent landscape of conflict and propaganda, terrorist organizations have increasingly relied on sophisticated communication strategies to project a powerful and appealing image to their target audiences. Among these strategies is the instrumentalization of brand archetypes, a concept originating in marketing and psychology, which allows organizations to create deeply resonant and symbolic representations of their ideals, goals, and missions. Brand archetypes are rooted in Carl Jung's theory of archetypes universal, recurring symbols or characters that appear across human culture and experience. Organizations use these archetypes to foster emotional connections, define their identity, and create a clear and relatable image. This tactic is particularly evident in the case of *Al-Dawla Al-Islamiya fi al-Iraq wa al-Sham* (Daesh), a globally recognized terrorist organization known for its extensive use of propaganda to recruit, radicalize and terrorize. Through carefully crafted narratives and symbolic imagery, Daesh has managed to create an influential organizational brand, appealing to a diverse range of disaffected individuals around the globe. The organization has employed several archetypes to align with its goals, such as the 'warrior' archetype to recruit fighters or the 'savior' archetype

---

The information and views expressed in this article are solely those of the author's and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer/s is affiliated.

1 Independent Researcher
2 Independent Researcher

to present itself as a defender of Islamic values and culture. The aim of this study is to analyze how terrorist organizations, particularly Daesh,

employ brand archetypes as strategic tools to design their organizational branding and to cultivate a powerful and persuasive image in the eyes of their target audiences. By examining the role of archetypes in Daesh's branding and propaganda, we can better understand how such groups use psychological and symbolic tools to extend their scope and influence. Through this approach, we explore the psychological appeal of these archetypes and how they contribute to Daesh's propaganda strategies and recruitment.

Keywords: *Brand Archetypes, Daesh, Propaganda, Recruitment, Perception.*

1. Introduction

In the contemporary interconnected world, brand archetypes significantly influence public perception and behavior, affecting both corporations and non-state entities, including terrorist organizations. Brand archetypes are based on Carl Jung's hypothesis of universal legendary figures that exist within the collective unconscious of individuals across cultures. This concept has been extensively utilized in marketing and branding to forge profound emotional ties with viewers (Tsai, 2006). Furthermore, beyond the scope of corporate branding, the impact of archetypes extends into political, social and even extremist spheres, where they are instrumental in shaping narratives, attracting followers and influencing public opinion. Terrorist organizations such as Daesh have employed brand archetypes to establish a distinct identity, cultivate a sense of allegiance among followers, and propagate their ideology. Terrorism functions as a form of political communication that significantly depends on symbols, visual media and narratives to attract attention, confer legitimacy and enlist new adherents (O'Shaughnessy & Baines, 2009). Comprehending the utilization of archetypal branding by these groups facilitates a deeper understanding of their recruiting and propaganda strategies, along with the efficacy of counter-narratives. This article seeks to examine how terrorist organizations employ brand archetypes to construct their identities, narratives, and techniques for recruitment and propaganda. The primary aims of this research are:

- Firstly, to analyze the function of brand archetypes in the communication strategies of terrorist organizations, with particular emphasis on their projection of specific archetypal images (e.g., Hero, Outlaw) to recruit and maintain adherents.
- Secondly, to investigate the efficacy of archetypes in communicating the

organization's objectives, principles, and identity to stakeholders, both internal (prospective recruitment) and external (global audiences).

- Thirdly, to evaluate the influence of brand archetypes on recruitment strategies, examining how organizations such as Daesh have adeptly employed archetypes to inspire action, convey a sense of purpose, and position themselves as leaders of a broader movement.
- Finally, to formulate strategic proposals for opposing these archetypal narratives using counter-narratives and communication techniques that may reduce the allure and perceived legitimacy of terrorist organizations.

2. The Notion of Brand Archetypes

2.1. Establishing Brand Archetypes

Brand archetypes originate from Carl Jung's archetypal theory, which posits that universally recognizable characters or symbols exist within the collective unconscious. Jung posits that archetypes are essential patterns or models of individuals, behaviors or personalities that persist across cultures and epochs, affecting perceptions and influencing thoughts and actions (Jung, 1954). These archetypes appear in narratives, mythologies and contemporary branding, serving as a psychological framework for brand perception and interaction (Bechter et al.,2016).

In branding, archetypes signify several personality characteristics that a business may adopt to establish a more profound emotional connection with its audience. Brands that correspond with a particular archetype adeptly engage subconscious associations and emotions that resonate with their intended audiences. The concept of brand and branding has a direct relationship with archetypes. A brand engages with mental imagery when analyzed cognitively. Therefore, image construction or image management is of great importance in branding processes. In this context, archetypes functionally come into play. Branding can be carried out at an individual, institutional, community and even national level. However, archetypes play an important role in all of these. In each branding process, the perception of the relevant unit and actor in line with the desired image from the external environment is related to the archetypes used. The perception of an individual, institution, community, or nation in accordance with the determined qualities (strength, adventurousness, wisdom, optimism, etc.) from the perspective of the identified target audiences strengthens and reinforces communication with those audiences. Through archetypes, the relevant target audiences can identify with the individual, institution, community or nation in question, and a cognitive bridge is established between the mass and the subject-actor through branding. (Mark & Pearson, 2001; Poon, 2016)

2.2. The Twelve Primary Archetypes

Jung's research led to the establishment of twelve fundamental archetypes, each embodying a unique personality and a specific set of traits. These archetypes function as foundational concepts for brand identification, allowing firms to embody their brand and develop a relatable image. The twelve archetypes and their shared characteristics are as follows (Jung, 1954):

The Innocent or Innocence: Embodies optimism, purity, and a yearning for happiness. Brands using this archetype seek to project sincerity and goodness, aiming to create a sense of trust and simplicity. Coca-Cola is often seen as embodied with this archetype, focusing on themes of happiness and togetherness.

The Sage: Represents wisdom, knowledge and a drive for understanding the world. Brands adopting the Sage archetype prioritize education, information and learning, often positioning themselves as thought leaders. Google is an example, as it aims to organize the world's information and make it accessible.

The Explorer: Embodies the desire for adventure, discovery, and freedom. Brands that identify with the Explorer encourage consumers to push boundaries and seek new experiences. Jeep, with its adventurous branding, taps into this archetype, symbolizing freedom and discovery. Pursues adventure, discovery, and autonomy.

The Outlaw (or Rebel): Embraces rebellion, disruption, and breaking the status quo. Brands using the Outlaw archetype often challenge the norms and encourage consumers to embrace their individuality. Harley-Davidson is a classic example of a brand that thrives on rebellion and individuality.

The Hero: Pursues achievement, courage, and bravery. Brands embodying the Hero archetype inspire consumers to take on challenges and strive for greatness. Nike, with its message of overcoming obstacles and pushing limits, is an embodiment of the Hero archetype.

The Lover: Driven by passion, intimacy, and connection. Brands adopting this archetype focus on creating emotional and aesthetic experiences for their audience, often linked with luxury, indulgence or beauty. Chanel, for instance, exemplifies the Lover archetype through its luxurious and romantic brand messaging.

The Jester: Focuses on bringing joy, humor, and light-heartedness. Brands using this archetype aim to entertain and lighten the mood, offering fun and amusement to their consumers. M&M's, with its playful and humorous advertising, reflects the Jester archetype.

The Caregiver: Represents compassion, care, and protection for others. Brands embracing the Caregiver archetype prioritize nurturing and safeguarding, often appealing to families or communities. Johnson & Johnson is an example,

positioning itself as a protector and caregiver for families' health.

The Creator: Desires innovation, creativity, and self-expression. Brands that identify with the Creator archetype focus on fostering creativity and empowering consumers to express themselves. Lego, which encourages creativity and building, is a prominent example of this archetype.

The Ruler: Associated with control, leadership and responsibility. Brands adopting the Ruler archetype position themselves as authoritative and in control, often projecting power and status. Luxury brands like Rolex or Mercedes-Benz often utilize the Ruler archetype, reflecting prestige and dominance.

The Magician: Focuses on transformation, imagination and making dreams a reality. Brands adopting the Magician archetype aim to create awe and wonder, often through innovation and change. Disney, with its enchanting storytelling and theme parks, embodies the Magician archetype by turning fantasy into reality.

The Everyman: Strives for belonging, authenticity and relatability. Brands using this archetype emphasize commonality and appeal to a wide audience, making them feel understood and part of a larger group. Ikea, known for offering affordable and practical home solutions, resonates with the Everyman archetype by positioning itself as accessible to all.

Each archetype represents a certain array of human aspirations and emotional experiences. Nike exemplifies the 'Hero' archetype, highlighting physical accomplishment and the ambition to surpass personal boundaries, while Coca-Cola frequently associates with the 'Innocent', advocating themes of joy and unity (Tsai, 2006).

2.3. Significance in Branding

The deliberate implementation of archetypes in branding significantly influences audience perception and engagement with a brand. By embodying an archetype, businesses leverage profound emotional and psychological connections, allowing them to differentiate themselves in a saturated market and cultivate enduring relationships with consumers. Ceballos and Villegas assert that the adoption of archetypes allows brands to cultivate a distinctive personality that aligns with certain audience values and goals, hence fostering robust brand loyalty and recognition (Ceballos & Villegas, 2015).

Aligning a brand with the Explorer archetype may resonate with customers who prioritize freedom and adventure, whereas adopting the Caregiver archetype might attract consumers who desire trustworthiness and caring attributes in a company. These psychological alignments render archetypal branding exceptionally potent, since they resonate with intrinsic human needs and emotions, resulting in deeper and more lasting customer experiences (Poon, 2016).

2.4. Archetypes as Catalysts for Emotional Engagement

Archetypes serve as emotional touchstones, influencing both brand perception and consumer emotional responses. The Hero archetype frequently evokes sentiments of empowerment and self-assurance, prompting consumers to resonate with the brand's narrative of strength and accomplishment. The Magician archetype evokes wonder and transformation, facilitating an aspirational journey for the consumer (Mark & Pearson, 2001)

The alignment of archetypes and emotional experiences is essential in storytelling and advertising, as brands aim to craft narratives that connect with their audience. The strategic application of archetypes in brand messaging and imagery can enhance customer affinity, engagement and advocacy. Emphasizing consistent archetypal traits, advertisers can develop campaigns that elicit strong emotions, hence reinforcing the brand's standing in the consumer's consciousness (Bechter et al., 2016).

2.5. Archetypes in Brand Strategy and Positioning

Archetypes are fundamental to brand strategy and positioning, offering a framework for a company's market presentation. This entails synchronizing a brand's mission, vision, and communication style with the selected archetype to continuously reinforce the intended image. This potent brand archetype functions as a 'brand portrait', influencing perceptions and directing strategic branding and marketing actions (Djakeli & Sheb, 2017).

By choosing an archetype that corresponds with the brand's fundamental principles and target demographic, organizations may tailor their communication, graphics and marketing techniques to continually reinforce the brand's archetypal identity. The Lover archetype frequently employs imagery and messaging that highlight beauty, connection, and intimacy, with the objective of establishing a profound emotional connection with the consumer (Jeffrey, 2025).

Brand archetypes offer an essential framework for establishing robust emotional connections between brands and consumers. By embracing a distinct archetype, brands may cultivate a definitive identity and narrative that aligns with their audience's psychological needs and aspirations. The strategic application of archetypes facilitates the development of memorable and engaging brands that cultivate loyalty, advocacy, and market distinction (Maidment, 2021).

3. Utilization of Brand Archetypes in Political and Extremist Settings

3.1. Expanding Brand Archetypes Beyond Commerce

Although brand archetypes are typically linked to corporate branding, their application is not confined to commercial pursuits. Archetypes can be utilized by any group or movement aiming to influence public image, establish a unified identity

and garner supporters. In politics, social movements, and extremist organizations, these archetypes function as frameworks that shape the group's perception, akin to conventional branding. The archetypes facilitate the creation of a narrative that resonates profoundly with the psychological and emotional dimensions of the target audience (Djakeli, 2017).

Political movements and extremist factions exploit archetypal constructs to develop narratives that align with their ideologies and objectives. The 'Hero' archetype frequently illustrates the organization as a virtuous savior or guardian against perceived dangers. Simultaneously, the 'Outlaw' archetype may be employed to depict the organization as a defiant entity confronting an oppressive regime. These archetypes are particularly efficacious since they engage universal narratives and emotions, enabling the organization to build a distinct and compelling narrative that resonates with the aspirations and grievances of its target audience (Seyle & Besaw, 2020).

In political circumstances, embracing a specific archetype might serve as a tactical response to contextual variables. During elections or political upheavals, parties or movements may adopt the 'rebel' archetype to galvanize discontent or the 'Caregiver' archetype to foster solidarity and support across communities. This strategic employment of archetypes enables groups to establish a favorable position within the political arena, impacting both allies and adversaries (Smith, 2016).

3.2. Narrative Authority in Extremist Organizations

Extremist organizations, akin to any institution, significantly depend on narrative, symbolism, and principles to construct an engaging identity that draws adherents. These tales are intricately connected to archetypes, aiding in the articulation of the organization's mission, vision, and societal function. Through the strategic utilization of archetypes, extremist organizations can elevate their status from marginal entities to recognized advocates of a cause, attracting individuals who identify with the group's story (Braouezec, 2016).

The 'Hero' figure frequently has a major role in extremist narratives, portraying the organization as valiant combatants against perceived adversaries or oppressors. Members are depicted as selfless warriors engaged in a noble cause, so legitimizing violent behavior and cultivating a sense of pride and glory among recruits. This heroic narrative can evoke a sense of obligation and purpose, motivating individuals to dedicate themselves to the organization's objectives and view themselves as integral to a broader, just cause (Obaidi et al., 2022).

The 'Outlaw' or 'Rebel' archetype is prominent in extreme narratives, especially when the group aims to portray itself as a challenger to a perceived corrupt or repressive system. Extremist organizations frequently portray themselves as

insurgents challenging an inequitable existing quo, attracting members who perceive themselves as disenfranchised or downtrodden. This archetype conjures notions of autonomy, rebellion and resistance, rendering the group's cause not just justified but imperative. Extremist organizations such as the English Defense League in the UK and the Bloc Identitaire in France have employed the 'Outlaw' archetype to consolidate members against perceived cultural and political challenges to national identity (Braouezec, 2016).

The 'Sage' and 'Magician' archetypes are utilized to construct a story of knowledge and transformational influence. The Sage archetype frequently appears in ideologies that prioritize profound knowledge, historical accounts, or philosophical reasoning to substantiate the group's convictions and behaviors. The Magician archetype embodies the capacity for change and transformation, providing followers with a sense of agency and the ability to influence their surroundings (Adamska, 2016).

3.3. Recruitment via Archetypal Narratives

Archetypes significantly influence the recruitment techniques of extremist organizations. By embracing a certain archetype, extreme groups can construct recruitment narratives that align with the distinct psychological needs and aspirations of prospective adherents. Individuals pursuing meaning, purpose or belonging may be attracted to the 'Hero' or 'Outlaw' archetypes, since they provide a framework for comprehending their role in the world and participating in a cause greater than themselves (Alizadeh et al., 2017).

Extremist organizations utilize narrative techniques to establish a compelling group identity that resonates with prospective recruits for example by framing participation as a heroic religious duty and an adventurous, meaningful life that promises belonging and romanticized lifestyle within a utopian so-called 'Islamic State' as seen in Daesh recruitment propaganda (Kharroub, 2015). Daesh adeptly employed storytelling to portray itself as the authentic protector of Islam, deploying heroic-martyr and outlaw style narratives that cast its fighters as defenders of an oppressed Ummah and as rebels against corrupt and unjust powers (Carter Center, 2016). Research on Daesh media shows that these heroic martyr narratives emphasize personal glory, empowerment and an exciting, elevated sense of purpose, while social martyr narratives stress religious obligation, sacrifice for the community, and moral duty (Cohen et al., 2024). This narrative framework is particularly effective in appealing to disenchanted individuals seeking meaning, adventure and belonging, thereby enhancing Daesh global recruitment potential by aligning its propaganda with underlying psychological needs and dispositions associated with attraction to extremism (Yoder et al., 2020).

Narrative engagement is the method by which archetypes influence individuals. Narrative engagement denotes the process via which humans resonate with the characters, frameworks, occurrences, and contexts embedded inside a narrative, thus relating to their own identity or life narrative. Consequently, when a narrative resonates with an individual, they can more readily embrace the cognitive framework it offers. Archetypes assume a significant role in this process. Archetypes significantly influence narrative involvement, shaping the elements with which individuals identify. An individual can recognize an actor inside a narrative and the accompanying stories through archetypes such as hero, outlaw, rebel, sage, etc., and can identify with these archetypes. This circumstance offers individual cognitive and emotional fulfillment. Consequently, archetypes are a fundamental component of narrative engagement and, by extension, of recruitment processes. Empirical research on Daesh propaganda shows that heroic and 'Outlaw'-style martyr narratives heighten narrative transportation and perceived recruitment appeal, particularly among individuals whose psychological dispositions align with these archetypal stories (Cohen et al., 2024). In this way, potential recruits interpret organizational narratives through archetypal lenses, align their self-concept with these narratives, and develop empathy and engagement toward the organization, thereby facilitating processes of radicalization and enlistment (Carter Center, 2017).

3.4. Symbolism and Brand Identity in Extremist Organizations

Symbols, colors, and language are essential in supporting the archetypal narrative of extremist groups. Similar to the ways in which private companies utilize visual aspects to strengthen their identity, extreme groups adopt emblems to resonate with their selected typology. The utilization of flags, insignia, and color schemes facilitates the establishment of the group's identification and conveys its objective succinctly. A black flag or emblem, for example, can signify the 'Outlaw' or 'rebel' archetype, whereas depictions of warriors or historical figures can bolster the 'Hero' archetype (Casiraghi & Cusumano, 2024).

Virtual communities are crucial for propagating these symbols and strengthening the group's archetypal story. Extremist organizations utilize forums, social media, and various online platforms to disseminate their narratives, enhance their brand identification, and foster a feeling of community among members. This strategy allows the group to sustain a cohesive message and engage with individuals beyond geographical borders, so augmenting their influence and reach (Benigni, 2017).

Brand archetypes transcend business and commercial branding, functioning as potent instruments for crafting narratives and identities in political movements and violent extremist organizations. By employing archetypes like the Hero, Outlaw,

Sage, or Magician, these groups create engaging narratives and symbols that resonate with their intended audience, facilitating the development of a unified identity and drawing in adherents. The efficacy of archetypes resides in their capacity to address profound psychological and emotional needs, facilitating extreme organizations in recruiting, inspiring, and mobilizing individuals for their agenda (Casiraghi & Cusumano, 2024).

4. Daesh and Brand Archetypes

4.1. Strategic Branding of Daesh

Daesh has adeptly utilized branding strategies to construct its image and narrative, incorporating both concrete and abstract components to distinguish itself from other extremist organizations. Daesh use political communication and propaganda to shape its perception, portraying itself not merely as a terrorist group, but as a legitimate political and social force (Simons, 2018). The group's branding emphasizes the projection of might, authority, and religious piety to establish credibility and authenticity within a saturated ideological marketplace (Simons, 2018).

By deliberately embracing brand stereotypes, Daesh may construct a story that appeals to its intended audience. It employs many media platforms, including magazines such as *Dabiq* and *Rumiyah,* social media, videos and music to strengthen its brand and engage varied audiences. The group's branding transcends its immediate operations to position itself as a 'perpetual' state-like organization, so enhancing its legitimacy and facilitating recruitment (Simons, 2018).

4.2. Utilized Archetypes in Daesh Propaganda

Daesh adeptly utilizes various archetypes to articulate its identity, principles, and mission, particularly the 'Hero' and the 'Outlaw, Sage, Innocent, Ruler and Caregiver'.

Daesh uses hero archetype as Daesh portrays itself in its propaganda as the 'Hero' safeguarding Islam and the Muslim community against perceived global injustices. This image aims to instill a sense of obligation and valor in recruits, portraying Daesh members as courageous combatants involved in a righteous cause. Daesh's media frequently features narratives of martyrdom and sacrifice, idealizing their warriors as religious heroes engaged in the pursuit of establishing the *Khalifah* (Caliphate) (Mahood & Rane, 2017).

The 'Outlaw' or 'rebel' persona is important to Daesh's narrative. It positions itself as a transformative organization confronting corrupt systems and opposing tyranny from Western governments and local authorities (Gerges, 2016). In its English-language videos and magazines, Daesh repeatedly positions itself as

the only uncompromising force willing to challenge 'apostate' rulers and global powers, thereby cultivating a sense of empowerment and moral superiority among followers who are invited to see themselves as rebels against injustice rather than mere criminals or extremists (Qi, 2024).

The 'Innocent' archetype serves as an additional archetype and instrument employed by Daesh. The Innocent archetype embodies innocence, blamelessness, virtue, and purity. In this context, Daesh ascribes these traits and attributes to itself. Consequently, Daesh portrays the organization collectively as a 'cohort of virtuous, impeccable, blameless adherents.' By branding the organization in this manner, Daesh can lead members to perceive it as a 'means of purification from sins and errors, and a route to achieving innocence.' Consequently, individuals may enlist in the group to pursue this objective (Carter Center, 2016; Gerges, 2016).

The 'Innocent' archetype, conversely, serves as an additional archetype and instrument employed by Daesh. The 'Innocent' archetype embodies innocence, blamelessness, virtue, and purity. In this context, Daesh ascribes these traits and attributes to itself. Consequently, DAESH portrays the organization collectively as a 'cohort of virtuous, impeccable, blameless adherents.' By branding the organization in this manner, Daesh can lead members to perceive it as a means of purification from sins and errors, and a route to achieving innocence. Consequently, individuals may affiliate with the organization in pursuit of this endeavor.

Another character employed by Daesh is the 'Caregiver' archetype. The 'Caretaker' archetype embodies service and nurturing. In this context, Daesh presents itself as an entity that provides a means of serving God and all Muslims to the populace by employing this archetype. Currently, Daesh is attempting to cultivate the notion that the avenue for Muslims to worship God is through allegiance to Daesh.

Taken together, these archetypal configurations - Hero, Outlaw/Rebel, and Innocent, complemented by elements of the Sage, Ruler, and Caregiver – enable Daesh to build a coherent, emotionally loaded brand identity. The Hero frame offers glory and purpose; the Outlaw/Rebel frame offers empowerment through transgression and radical purity; and the Innocent frame offers moral absolution and spiritual renewal. This archetypal repertoire does not merely ornament Daesh's ideology; it structures how audiences are invited to feel, think, and act in relation to the group's project (Atwan, 2015).

4.3. Tactics and Utilization of Media

The utilization of media by Daesh is a vital component of its branding strategy, enabling the group to spread widely its narrative and sway potential recruits. The organization utilizes advanced media strategies across multiple platforms to strengthen its selected archetypes.

Daesh is recognized for its meticulously crafted movies, photos, and online propaganda initiatives that use social media platforms such as Twitter (officially known as X since 2023), YouTube and Telegram. This propaganda emphasizes the material, spiritual and social advantages of joining Daesh enhances online support for the organization, whereas content depicting extreme violence elicits more ambivalent responses – enthusiasm from core supporters and aversion from the broader audience (Mitts et al., 2021). This equilibrium in substance sustains allure for prospective recruits while simultaneously instilling apprehension in adversaries (Mitts et al., 2021).

Daesh uses storytelling in its propaganda to establish emotional ties with its intended audience. Daesh's media disseminate meticulously constructed narratives that depict themes of heroism, sacrifice, and adventure, resonating with the personal aspirations and desire of prospective recruits (Kruglova, 2020). Daesh adeptly employs narrative advertising to humanize its combatants and build a robust connection with its intended audience, hence augmenting the group's efficacy in disseminating its ideologies (Kruglova, 2020).

Daesh has created various online periodicals, including *Dabiq* and *Rumiyah*, aimed at solidifying its brand identity and disseminating its message to both English- and non-English-speaking audiences. These periodicals are expertly crafted, showcasing aesthetically pleasing design, superior imagery, and engaging narratives. The text underscores themes of religious obligation, the valor of jihad and the organization's political objectives, thereby legitimizing Daesh's activities and motivating adherents.

Daesh use Islamic chants referred to as *nasheeds* as a component of their propaganda efforts. These *nasheeds* elicit emotion and foster solidarity among consumers, strengthening the themes of war, sacrifice and triumph. These chants are frequently employed in movies that convey strength and religious themes, so reinforcing the group's portrayal as a divine entity advocating for a just cause (Yarchi, 2019).

The brand archetypes of Daesh are crucial in shaping the group's identity and narrative. Daesh adeptly employs storytelling, symbols and media to attract, motivate and mobilize adherents by presenting itself as a 'Hero' protecting Islam, an 'Outlaw' resisting persecution and a religious 'Sage' offering spiritual direction. The group's utilization of digital channels, visual propaganda and narrative marketing amplifies its capacity to project authority, garner support and sustain a cohesive brand identity among diverse audiences.

5. Influence of Brand Archetypes on Recruitment and Perception

5.1. Psychological Persuasion

The archetypes utilized by extremist organizations such as Daesh exploit the profound psychological needs and aspirations of its intended audience. These requirements encompass a sense of belonging, importance, defiance, and valor. The 'Hero' archetype caters to the yearning for purpose and bravery, portraying the group's endeavors as honorable and just. The depiction of battling perceived injustices appeals to an individual's desire to seek significance and engage in a broader, heroic endeavor (Abumelhim, 2023).

The 'Outlaw' character attracts individuals who desire to revolt against a corrupt or oppressive society. This character fosters empowerment and resonates with sentiments of marginalization or disaffection. Organizations such as Daesh have effectively employed these narratives to elicit emotional reactions that render their cause seemingly justifiable and attractive, offering psychological advantages to recruits attracted to these themes (Obaidi et al., 2022).

The psychological allure also encompasses presenting the battle as a pursuit of meaning, wherein individuals perceive their actions as contributing to a spiritual or historical objective. The 'quest for significance' idea posits that the yearning for importance is fundamentally embedded in an individual's psychological constitution and can be stimulated by extreme narratives to rationalize and promote involvement in political violence (Jasko et al., 2020).

5.2. Recruitment Efficacy

The purposeful utilization of archetypes by extremist organizations profoundly impacts recruitment, public perception and fundraising initiatives. By aligning their operations with the Hero archetype, Daesh provides a compelling attraction for anyone desiring to participate in a purportedly noble cause. This renders the group's endeavors as demonstrations of bravery and selflessness, which can be especially enticing for young people in search of adventure, honor and meaning in their life.

Furthermore, the 'Adventurer' archetype capitalizes on individuals' yearning for exhilaration and risk, resonating with those drawn to the notion of participating in battle or revolutionary endeavors. According to Obaidi, the Extremist Archetypes Scale, which delineates characteristics such as the 'Adventurer', 'Drifter' and 'Leader' inside extremist groups, emphasizing the distinct psychological profiles that these sub-groups seek in their recruitment strategies (Obaidi et al., 2022).

The employment of archetypes such as the 'Hero' and 'Outlaw' in branding has demonstrated efficacy as a recruitment technique for Daesh. The 'Hero' archetype resonates with people pursuing adventure, honor, and the pursuit of a just cause, whereas the 'Outlaw' archetype captivates those inclined towards revolt, anti-establishment ideologies, and a propensity to defy authority. These archetypes furnish recruits with a robust feeling of identity and purpose, affirming their decision to affiliate with this extremist organization (Obaidi et al., 2022).

There is correlation between distinct psychological profiles and the diverse motivations for joining extreme groups. Some individuals may be attracted to adventure and excitement, while others may be motivated by ideological conviction or a desire for belonging. Comprehending these archetypes enables extremist organizations to customize their propaganda and recruitment strategies to resonate with various psychological reasons (Obaidi et al., 2022).

The efficacy of these archetypes is seen in their capacity to resonate with diverse psychological demands. Extremists present their cause as a transformative conflict against perceived adversaries, providing recruits an opportunity to change their lives and achieve a greater purpose. Moreover, narratives concerning martyrdom and the struggle for a divine cause serve to support the Hero archetype and legitimize the employment of violence as a permissible method to achieve their objectives (Speckhard et al., 2019).

5.3. Counter-Narratives and Competing Archetypes

Effectively countering extremist narratives necessitates comprehending and utilizing competing archetypes to contest the ideas and narratives propagated by Daesh. One strategy is to present alternative narratives that explicitly refute the messaging of radicals by characterizing them as duplicitous, cowardly, or manipulative. The objective is to undermine the allure of the Hero or Outlaw archetypes by revealing inconsistencies or by highlighting counter-topics such as peace, democracy, and communal harmony.

Research by Bélanger and colleagues indicates that counter-narratives can effectively diminish support for extremist ideologies; nevertheless, their efficacy is contingent upon criteria such as content, source, and the psychological characteristics of the audience. The research indicates that political counter-narratives were the most efficacious, particularly when presented by credible figures such as defectors, who can directly contest the group's legitimacy (Belanger et al., 2020).

Another technique involves utilizing internet games and media initiatives to foster resistance against extremist narratives. This innovative method for counter-narrative efforts employs themes and messages that contest the archetypes employed by extremists, promoting critical thinking and diminishing the psychological allure of extremist material (Pisoiu & Lippe, 2022).

Nonetheless, counter-narratives present difficulties as well. Strategic communication and content moderation on social media require meticulous management, as efforts to resist extreme information may inadvertently reinforce it or incite reaction. The research advocates for a sophisticated strategy in content moderation and underscores the necessity of collaborative efforts among several stakeholders to successfully combat extremist narratives while safeguarding free speech (Ganesh & Bright, 2020).

Another difficulty with counter-narratives is their efficacy among individuals already susceptible to radicalization. Bélanger discovered that counter-narratives may exert only a marginal effect on diminishing support for Daesh among those with a high susceptibility to radicalization. They propose that political and social narratives are more impactful than religious narratives, and that the origin of the message (e.g., Daesh defectors) might significantly affect the reception of the counter-narrative. For people firmly embedded in extremist ideas, exposure to counter-narratives may occasionally strengthen their allegiance to the group due to reactance or a perceived assault on their convictions (Belanger et al., 2020).

Counter-narrative techniques must also consider psychological profiles. The research indicates that those with a pronounced desire for social significance are more inclined to engage with extremist narratives, particularly in radical social environments. Consequently, effective counter-narrative efforts must tackle these psychosocial vulnerabilities by offering alternative avenues to significance and belonging (Jasko et al., 2020).

Initiatives to combat extremist narratives utilize alternative archetypes to present diverse avenues for meaning and purpose. Counter-narratives may depict government officials or peace-building organizations as ‘Heroes’ or ‘Sages’, providing knowledge, stability, and avenues for constructive transformation (Pisoui & Lippe, 2022). Notwithstanding these endeavors, the efficacy of counter-narratives can be inconsistent, especially when they fail to align with the personal experiences and emotions of the intended audience. Consequently, developing persuasive counter-archetypes that cater to the psychological needs and social settings of those susceptible to radicalization is essential for undermining the influence of extremist propaganda.

6. Obstacles and Ethical Considerations

6.1. Abuse and Exploitation of Archetypes

Brand archetypes are potent instruments that can be misappropriated by violent organizations, resulting in recruitment, radicalization, and the dissemination of extremist ideology. Extremist organizations utilize archetypes to construct persuasive narratives and influence emotions and perceptions to further their objectives. The ethical dilemma arises from the appeal of these archetypes to fundamental psychological desires, including affiliation, heroism, and rebellion, rendering humans susceptible to manipulation and exploitation.

Tilley proposed the 'propaganda index' to evaluate the ethicality of message communication. The index assesses the presence of stylistic components typically recognized as propagandistic and applies this evaluation to case studies of terrorism-related discourse. The findings underscore that elevated levels of propaganda in communication may not successfully fulfill objectives in an ethical or efficient manner (Tilley, 2005).

Archetypes significantly influence identities and narratives; yet extremist organizations frequently exploit them to bolster 'us versus them' mentalities, incite violence, and rationalize terrorism as a moral imperative. The 'Hero' archetype might exalt martyrdom, but the 'Outlaw' archetype may advocate for revolt and defiance against authority, framing violent activities as a virtuous resistance to injustice. The use of archetypes profoundly influences the psyche of adherents and recruits, frequently resulting in radicalization.

6.2. Challenges in Counter-Terrorism Communication

Governments and counter-terrorism agencies encounter substantial hurdles in combating archetype-based propaganda, as they must consider the ethical ramifications of their messaging while striving to delegitimize extremist ideologies. The balancing effort entails honoring free expression while simultaneously restricting the dissemination of perilous ideology.

Sabir contends that counter-terrorism initiatives, including the UKs Pursue and Prevent policies, obscure the distinction between compulsion and agreement. These techniques entail the targeting of propaganda, resulting in comprehensive surveillance that may occasionally erode the trust and social inclusion the government seeks to foster. This generates a paradox in which attempts to thwart terrorism may unintentionally result in further alienation and radicalization (Sabir, 2017).

The media has a responsibility in the ethical transmission of knowledge about terrorism, highlighting the challenges that emerge from news being simultaneously a business and a social commodity. Terrorist organizations frequently exploit media outlets to enhance their narratives, while counter-terrorism authorities confront the dilemma of managing the ethical ramifications of media reporting without compromising journalistic autonomy (Schmid, 1989).

With the technological era we see, the increasing sophistication of cyber-terrorism, which uses online propaganda to sway and attract susceptible individuals. The scholars contend that counter-terrorism efforts must integrate online surveillance with proactive counter-communication to successfully disrupt extremist messaging. The difficulty is to guarantee that counter-terrorism measures are both legally valid and ethically suitable in reconciling privacy, freedom of expression and national security (Palasinski & Bowman-Grieve, 2017).

The difficulties in addressing archetype-based messaging are complex. The use of archetypes by terrorist organizations engenders ethical issues, resulting in the radicalization and manipulation of individuals. Simultaneously, counter-terrorism communication encounters the challenge of effectively deconstructing extremist narratives while adhering to ethical standards and human rights. The equilibrium between countering propaganda and safeguarding free speech and democratic principles constitutes a significant tension in evaluating the ethical ramifications of branding methods employed by both terrorists and counter-terrorism entities.

7. Strategic Proposals

Counter-terrorism tactics must effectively utilize brand archetypes to construct persuasive counter-narratives that can undermine extremist messaging. Effective counter-narratives must be genuine, pertinent, and tailored to the specific circumstances of the intended audience. The motives and psychological demands of prospective recruits are essential for formulating impactful messaging. Counter-narratives must supplant extremist narratives by addressing analogous emotional and social demands, offering alternative avenues for belonging, meaning and purpose (Beutel et al., 2016).

Counter-narratives utilizing the personal accounts of former extremists, who articulate their disappointment with groups such as Daesh, have demonstrated efficacy. These testimonies foster relatability and humanize the ramifications of radicalization, undermining the allure of extremist stereotypes like the ‘Hero’ or ‘Outlaw’ (Speckhard et al., 2019).

Given the prevalence of online platforms among young individuals, counter-narratives conveyed through gaming can foster resilience against extremism. Pisoiu and Lippe delineate the DECOUNT project, which created a game

integrating counter and alternate narratives. The project effectively engaged users by comprehending radicalization processes and the preferences of the target demographic, as well as utilizing channels like Instagram and YouTube, thereby addressing their experiences and countering extremist messaging (Pisoui & Lippe, 2022).

A framework introduced by Ingram endorses a two-tiered strategy that caters to various audience incentives. The initial tier endeavors to dismantle fundamental reasoning within extremist ideologies and propose alternative answers, whereas the subsequent tier focuses on disrupting the support and engagement networks around extremist organizations. This method facilitates a focused reaction that dismantles extremist ideology and undermines recruitment channels (Ingram, 2016).

Media organizations and social platforms are essential in overseeing and addressing the utilization of brand archetypes in extremist propaganda. A vital component of counter-extremism initiatives is contesting extremist perspectives on social media platforms. Counter-narratives should be deliberately disseminated across several platforms to engage varied audiences, considering the user behavior specific to each platform. This necessitates cooperation among governments, civil society, and technology firms to develop and disseminate content that mitigates the impact of extremist narratives (Van Eerten et al., 2019).

Content moderation on social media platforms requires a systematic methodology to combat extreme propaganda while preventing the infringement of free speech. It is essential to ensure that counter-narratives do not unintentionally enhance extremist propaganda or incite reaction (Ganesh & Bright, 2020).

Another study investigates how extremists employ ‘conspiratorial narratives’ to incorporate archetypal figures and events as a rationale for violence. Media platforms must acknowledge these tendencies to enhance their comprehension of how extremist narratives are constructed and to pinpoint appropriate intervention and disruption strategies (Baele, 2019).

Conclusion

This research examines the utilization of brand archetypes by extremist organizations such as Daesh, highlighting their significant influence on narrative construction, recruitment strategies, and public perception. Utilizing globally acknowledged archetypes like the ‘Hero’ and the ‘Outlaw’. These groups construct narratives that resonate with psychological demands including belonging, purpose, and rebellion. Daesh adeptly utilize these archetypes to cultivate a robust sense of identity and legitimacy, hence enhancing recruitment and solidifying their objectives.

We analyzed how Daesh deliberately employs brand archetypes to cultivate a persuasive image and recruit individuals, utilizing diverse media strategies such as social media, propaganda publications, and visual symbolism. The study examined the substantial obstacles faced by governments and counter-terrorism organizations in combating these archetypes, navigating the intricacies of strategic communication, freedom of speech, and the moderation of internet content without inadvertently enhancing extremist ideas.

An essential insight is that archetypes serve as both a structure for extremist narratives and a means for developing counter-narratives. To effectively combat extremist propaganda, counter-terrorism programs must utilize alternative archetypes that contest extremist narratives while providing avenues for fulfillment, belonging, and purpose through non-violent methods.

Daesh have proven adept at 'instrumentalizing brand archetypes' to craft a 'symbolically powerful and emotionally resonant identity'. By employing the 'Warrior', 'Savior', and 'Rebel' archetypes, Daesh provides a 'clear, compelling narrative' that taps into universal psychological needs. This strategy allows the group to recruit effectively across different cultures and demographics, offering individuals a 'sense of purpose, identity, and belonging' within a broader ideological framework.

The use of archetypes in terrorist propaganda is a reminder that these groups are not just violent extremists; they are 'ideological movements' that understand how to manipulate 'symbolic communication' to achieve their goals. The success of these efforts highlights the need for counterterrorism strategies to focus not just on military or law enforcement responses, but also on 'countering the narratives' that make these groups appealing in the first place.

Comprehending branding and archetypes within the realm of extremist propaganda offers essential insights into the methods these groups utilize for communication, recruitment, and image construction. Identifying these branding methods is crucial not only for evaluating terrorist propaganda but also for developing effective defenses. By incorporating these insights, governments, NGOs and counter-terrorism agencies can develop persuasive counter-narratives that diminish the allure of extremist groups, provide alternative avenues for individuals susceptible to radicalization, and ultimately foster a more informed and resilient society.

References

Abumelhim, M., Abu-Melhim, A. H., Rababah, M. A. I., & Rababah, K. A. (2023). Linguistic analysis of Daesh's miscontextualisation of the Quranic verses: Propaganda strategy. Journal of Language and Communication, *10*(2), 167–181. https://doi.org/10.47836/jlc.10.02.02

Adamska, M. (2016, July 25). What are brand archetypes? Part 1 – The Ruler, the Hero and the Outlaw. BrandStruck. https://brandstruck.co/blog_post/brand-archetypes-part-1-ruler-hero-outlaw/

Alizadeh, M., Weber, I., Cioffi-Revilla, C., Fortunato, S., & Macy, M. (2017). Psychological and personality profiles of political extremists. 1-24., arXiv preprint arXiv:1704.00119.

Atwan, A. B. (2015). Islamic State: The digital caliphate. Saqi Books.

Baele, S. J. (2019). Conspiratorial Narratives in Violent Political Actors' Language. Journal of Language and Social Psychology, 38(6), 706-734.

Bechter, C., Farinelli, G., Daniel, R.-D., & Frey, M. (2016). Advertising between Archetype and Brand Personality. Administrative Sciences, 6(2), 5., 1-11.

Bélanger, J., Nisa, C., Schumpe, B. M., Gurmu, T., Williams, M. J., & Putra, I. E. (2020). Do Counter-Narratives Reduce Support for Daesh? Yes, but Not for Their Target Audience. Frontiers in Psychology, 11:1059, 1-11.

Benigni, M. (2017). Detection and Analysis of Online Extremist Communities (Doctoral dissertation, Carnegie Mellon University, USA).

Beutel, A. J., Weine, S., Saeed, A., Mihajlovic, A., Stone, A., Beahrs, J., & Shanfield, S. (2016). Guiding Principles for Countering and Displacing Extremist Narratives. Journal of Terrorism Research, 7(1), 35-49.

Braouezec, K. (2016). Identifying Common Patterns of Discourse and Strategy among the New Extremist Movements in Europe: The Case of the English Defence League and the Bloc Identitaire. Journal of Intercultural Studies, 37(6), 637–648.

Carter Center. (2016). Religious appeals in Daesh's recruitment propaganda. The Carter Center. PDF

Carter Center. (2017). Daesh meta-narratives: From the global ummah to the hyperlocal. The Carter Center. PDF

Casiraghi, M. C. M., & Cusumano, E. (2024). Lethal brands: Terrorist groups' logos and violence. Journal of Peace Research, 61(x), 1–15. Abstract

Ceballos, L. M., & Villegas, J. (2015). Use of archetypes in the Colombian fashion industry. Estudios Gerenciales, 30, 195.

Cohen, M. S., Leong, Y. C., Ruby, K., Pape, R. A., & Decety, J. (2024). Intersubject correlations in reward and mentalizing brain circuits separately predict persuasiveness of two types of Daesh video propaganda. Scientific Reports, *14*, 13455. https://doi.org/10.1038/s41598-024-62341-3 Article

Djakeli, K. (2017). When the Brand is Losing its Archetypes it Dies Georgian Political Marketing at Elections. Journal of Business, 6(1), 17-20.

Djakeli, K., & Sheb, T. R. U. E. (2017). What is Brand Archetype Portrait (BAPOR) and How to Calculate Brand Archetype Power (BAPOW). Journal of Business, 6(1), 27-32.

Ganesh, B., & Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. Policy & Internet, 12(1), 6-19.

Gerges, F. A. (2016). DAESH: A history. Princeton University Press.

Ingram, H. J. (2016). A “Linkage-Based” Approach to Combating Militant Islamist Propaganda: A Two-Tiered Framework for Practitioners., 1-21.

Jaśko, K., Webber, D., Kruglanski, A., Gelfand, M., Taufiqurrohman, M., Hettiarachchi, M., & Gunaratna, R. (2020). Social context moderates the effects of quest for significance on violent extremism. Journal of Personality and Social Psychology, 1-23., http://dx.doi.org/10.1037/pspi0000198.

Jeffrey, S. (2025, August 16). *Brand archetypes: How to apply archetypal psychology to branding and marketing (12+ examples)*. Center for Leadership Studies. https://scottjeffrey.com/12-brand-archetype-wheel/

Jung, C. G., 1954 (Published 1981), The Archetypes and the Collective Unconscious, Collected Works, 9 (2nd ed.). Princeton, NJ: Bollingen, 44.

Kharroub, T. (2015, September 25). Understanding violent extremism: The social psychology of identity and group dynamics. Arab Center Washington DC. https://arabcenterdc.org/resource/understanding-violent-extremism-the-social-psychology-of-identity-and-group-dynamics/

Kruglova, A. (2020). “I Will Tell You a Story about Jihad”: Daesh’s Propaganda and Narrative Advertising. Studies in Conflict & Terrorism, 44(1), 115-137.

Mahood, S., & Rane, H. (2017). Islamist narratives in Daesh recruitment propaganda. The Journal of International Communication, 23(1), 15-35.

Maidment, A. (2021, August 23). *What are brand archetypes and why are they important? * March Branding. https://marchbranding.com/design-insight/brand-archetypes

Mark, M. & Pearson, C. S. (2001). The Hero and the Outlaw: Building Extraordinary Brands Through the Power of Archetypes. New York: McGraw-Hill.

Mitts, T., Phillips, G., & Walter, B. F. (2021). Studying the Impact of Daesh Propaganda Campaigns. The Journal of Politics, 84(3), 1220-1225.

Obaidi, M., Skaar, S. W., Ozer, S., & Kunst, J. R. (2022). Measuring extremist archetypes: Scale development and validation. PloS One, 17(7), e0270225., 1-29. https://doi.org/10.1371/journal. pone.0270225

O’Shaughnessy, N., & Baines, P. (2009). Selling terror: The symbolization and positioning of Jihad. Marketing Theory, 9(3), 227-241.

Palasinski, M., & Bowman-Grieve, L. (2017). Tackling cyber-terrorism: Balancing surveillance with counter-communication. Security Journal, 30(4), 556-568.

Pisoiu, D., & Lippe, F. (2022). The name of the game: Promoting resilience against extremism through an online gaming campaign. First Monday, 27(5). doi: https://dx.doi.org/10.5210/fm.v27i5.12600

Poon, S. T. F. (2016). Designing the brand archetype: Examining the role of Jungian collective unconscious in the creative customisation of brands. The International Journal of Social Sciences and Humanities Invention, 3(6), 2228–2239. https://doi.org/10.18535/ijsshi/v3i6.6

Qi, Y. (2024). Propaganda in focus: Decoding the media strategy of Daesh. Humanities and Social Sciences Communications, 11, Article 1123.

Sabir, R. (2017). Blurred lines and false dichotomies: Integrating counterinsurgency into the UK’s domestic ‘war on terror’. Critical Social Policy, 37(2), 202-224.

Schmid, A. (1989). Terrorism and the media: The ethics of publicity. Terrorism and Political Violence, 1(4), 539-565.

Seyle, C., & Besaw, C. (2020). Identity, extremism, and (de) radicalization. The Psychology of Extremism, 47-81.

Simons, G. (2018). Brand Daesh: Interactions of the Tangible and Intangible Environments. Journal of Political Marketing, 17(3), 322-353.

Smith, N. (2016, June 7). Brand archetypes — Meet the Outlaw. n-Vision Designs. https://nvision-that.com/brand-archetype-the-outlaw/

Speckhard, A., Shajkovci, A., & Ahmed, M. (2019). Intervening in and Preventing Somali-American Radicalization with Counter Narratives: Testing the Breaking the Daesh Brand Counter Narrative Videos in American Somali Focus Group Settings. Journal of Strategic Security. 11 (4), 32-71.

Tilley, E. (2005). Responding to terrorism using ethical means: The propaganda index. Communication Research Reports, 22(1), 69-77.

Tsai, S. (2006). Investigating archetype-icon transformation in brand marketing. Marketing Intelligence & Planning, 24(6), 648-663.

Van Eerten, J., Doosje, B., Konijn, E., de Graaf, B., & de Goede, M. L. (2019). Challenging Extremist Views on Social Media, Routledge Press.

Yarchi, M. (2019). Daesh's media strategy as image warfare: Strategic messaging over time and across platforms. Communication and the Public, 4(1), 53-67.

Yoder, K. J., Ruby, K., Pape, R., & Decety, J. (2020). EEG distinguishes heroic narratives in Daesh online video propaganda. Scientific Reports, *10*, 19593. https://doi.org/10.1038/s41598-020-76711-0 Article

Defence Against Terrorism
Review DATR Magazine

DATR, 2025; 2 : 49-72
Electronic Online ISSN 1307 - 9190

Beyond the Euro-Atlantic: Colombia's Path to NATO Global Partnership

Assoc.Prof.Dr.Başar Baysal[1*]

Abstract

NATO's evolution from a Euro-Atlantic defense bloc to a global security actor is evident in its partnership with Colombia, its first Latin American Global Partner. Central is counter-terrorism, given non-traditional threats like insurgencies and narcotrafficking. Colombia's counter-insurgency experience against FARC and ELN offers NATO valuable intelligence-based targeting and operational insights. NATO, in turn, benefits from Colombia's lessons in demining and illicit-economy disruption, enhancing its capacity for global security. This article examines key milestones – such as the 2013 Security of Information Accord – culminating in Colombia's Global Partner status in 2017. Drawing on neoliberal institutionalism, realism, and constructivism, it highlights how institutional incentives, strategic calculations, and norm diffusion collectively shape the alliance. Through Building Integrity and standardized training, NATO helps Colombia reduce corruption risks and improve military education. Realist factors enhance Colombia's deterrence in a region influenced by competing powers, while constructivist elements embed democratic oversight, ethics, and human rights in Colombia's defense culture. Consequently, synergy in counter-terrorism training fosters more robust intelligence-sharing channels and integrated responses to hybrid threats at domestic and international levels. Collaboration spans cyber defense, institutional reform, maritime security, and especially counter-terrorism. Yet, budget limits and domestic security challenges constrain deeper interoperability. Despite obstacles,

new capacity-building and intelligence-sharing initiatives illustrate how a post-conflict state can harness NATO's frameworks to modernize and contribute specialized counter-terrorism expertise. This partnership underscores evolving alliance models – flexible, interest-driven, and adaptive to global threats – demonstrating how Colombia's transition from conflict to regional actor aligns with NATO's shift toward broader security engagements. Such outcomes highlight international alliances' role in security.

Keywords

Colombia–NATO partnership, Counter-terrorism, Cooperative security, Post-conflict reform, Alliance theory

1. Introduction

NATO's evolution from a strictly Euro-Atlantic defense organization into a global security actor has become increasingly evident in the past two decades. Once limited to collective defense obligations among North American and European allies, NATO has been compelled by contemporary threats – terrorism, cyber espionage, and transnational organized crime – to develop strategic partnerships with countries outside its traditional region (Palma, 2025; Helbig & Lasconjarias, 2017). In this broader outreach, Colombia stands out as NATO's first Latin American global partner, a milestone that has introduced new dynamics into both Colombian security policy and NATO's global partnership framework. Scholars highlight the significance of this development for Colombia, which emerged from a decades-long internal conflict and sought to modernize its Armed Forces, as well as for NATO, which has been extending its network of cooperative security relationships (González Martínez et al., 2022). The Colombia–NATO partnership thus captures how alliances can be reconfigured in an era marked by cross-border threats like terrorism and the need for flexible collaborations.

The partnership gradually solidified through a series of agreements, including the 2013 Security of Information Accord and subsequent cooperation programs. For NATO, engaging Colombia offered a partner with valuable counter-terrorism experience and capacity in anti-narcotics, humanitarian demining, maritime security and, increasingly, cyber defense. For Colombia, cultivating close ties with the Alliance presented a pathway to institutional reform, advanced training initiatives, and renewed diplomatic leverage, especially in the aftermath of its 2016 Peace Accord with the FARC (Palma, 2025). According to Palma (2025), this partnership allowed Colombia not only to modernize its defense sector but also provided NATO with valuable insights into combating irregular warfare and

organized crime, areas where Colombia has developed substantial expertise. In a post-conflict setting, adopting NATO standards and participating in Alliance-run programs appeared to accelerate modernization within the Colombian Armed Forces while reinforcing Colombia's credibility as a global security contributor.

This partnership also raises fundamental inquiries for alliance theory. How does an alliance originally tailored to Europe's collective defense adapt to incorporate a Latin American state with substantial internal security imperatives? Does Colombia's model of partial integration, which excludes Article 5 obligations, illustrate a new template for cooperative security? Previous research has predominantly focused on U.S.–Colombia security ties or Colombia's peace process (McKellips, 2024; Rosas Garavito, 2021). Far less attention has been given to the concrete policy frameworks and implications of Colombia–NATO collaboration, including how it affects regional geopolitics and underscores theoretical insights on neoliberal institutionalism, realism, and constructivism. By filling these gaps, this article illuminates how NATO's emphasis on flexible partnerships resonates with Colombia's evolving defense profile.

Methodologically, the study draws on NATO publications, as well as academic literature in both English and Spanish, mapping the development of Colombia–NATO cooperation against the backdrop of shifting security concerns. It situates new initiatives – whether cyber defense and counterterrorism workshops, advanced training in counter-terrorism, or cooperative maritime missions – within the context of ongoing institutional reforms and budgetary constraints in Colombia. Structurally, this article first outlines the theoretical underpinnings that anchor NATO's global outreach, then traces key milestones in the partnership's expansion, highlighting five principal fields of collaboration. It then discusses how these arrangements compare to NATO's experiences with other global partners, drawing out the unique challenges Colombia faces as a post-conflict state with significant domestic vulnerabilities. Finally, it offers an up-to-date assessment of future prospects and policy recommendations, including deeper forays into research-based initiatives on the nexus of illicit economies, terrorism and emerging digital threats.

Taken together, the analysis contends that Colombia's engagement with NATO attests to the Alliance's growing need to forge new relationships beyond its historical theaters of operation, while showcasing how a Latin American military institution can tap external frameworks to modernize and gain international standing. It embodies a broader tendency in global security governance where alliances and partnerships become more fluid, relying less on formal treaty commitments and more on targeted, context-specific collaboration. Colombia's experience, from navigating internal reforms to contributing niche expertise in counterterrorism and demining, illustrates both the promise of and the friction within such cooperative

security strategies, highlighting that even as NATO expands its reach, it must accommodate the local realities and regional sensitivities of each new partner.

2. Theoretical and Conceptual Perspectives on NATO's Global Partnerships

NATO's contemporary positioning as a global security actor emerged out of a long history of adaptation from its original Euro-Atlantic defense remit to a more expansive cooperative security approach. Scholars have shown that in the aftermath of the Cold War, NATO began to transcend its core geographical boundaries, establishing strategic links with countries outside the Euro-Atlantic space (NATO, 2022). This shift was partly fueled by the recognition that new threats – ranging from transnational terrorism to cyber-attacks – could not be contained solely through regional alliances but required forging functional relationships with nations that possess relevant expertise or strategic locations (Clavijo Piñeros, 2017). Within this broader global orientation, Colombia became NATO's first Latin American partner, an association that illuminates the transformation of NATO's mission and compels theoretical examination of how international alliances are reconfigured in an era of interdependent security.

- NATO and Cooperative Security

Over the past two decades, NATO's Strategic Concepts have emphasized "cooperative security," an approach that treats partnership-building as integral to sustaining international order. Initially founded to ensure collective defense in the Euro-Atlantic arena, NATO gradually discovered that terrorism, narcotics trafficking, and cyber threats often originated beyond its traditional geographic perimeter (NATO, 2022). This realization led to various partnership programs with non-member states, particularly after the 2010 Strategic Concept, which named cooperative security as one of the Alliance's "core tasks" (NATO, 2010, p. 8). Cooperative security means broadening deterrence strategies beyond purely military measures, incorporating intelligence-sharing, institutional reform, cyber defense, and crisis management training with external partners (Clavijo Piñeros, 2017). Such initiatives aim to project stability rather than mere containment, reflecting an outlook that sees institutional cooperation as vital to preventing the spillover of conflicts.

Several authors point out that the impetus for forging "global partnerships" was closely tied to the challenges NATO faced in missions like Afghanistan, where non-traditional allies provided essential support (Helbig & Lasconjarias, 2017). Colombia's subsequent integration into NATO's partnership framework illustrates how the Alliance tapped into a state whose military's decades-long fight against terrorist groups and drug cartels offered a unique skill set (González Martínez et

al., 2022). Yet this expansion also revitalized questions about NATO's function – whether it remained a collective defense pact or had evolved into an international security network bridging multiple continents (Arciniegas & Dos Santos Filho, 2019). Cooperative security, in that sense, incorporates both deterrence and capacity-building. It retains the classic deterrence posture against adversaries but couples it with institutional frameworks designed to strengthen partner states' own security architectures (McKellips, 2024). The case of Colombia thus highlights NATO's simultaneous engagement in deterrence, containment, and multilateral cooperation.

- **Evolving Core Concepts: Deterrence, Containment, and Cooperative Security**

Deterrence remains at the heart of NATO's security philosophy, but the notion now extends beyond the conventional scenario of deterring aggressor states to include deterring transnational threats that blur lines between internal and external security (Arciniegas & Dos Santos Filho, 2019). Colombia's partnership demonstrates how deterrence can involve training programs that boost a partner's capacity to deter non-state actors, such as non-state armed groups. Containment, on the other hand, has historically referred to blocking adversaries' ideological and military expansion, a concept integral to NATO's early Cold War mission (González Martínez et al., 2022). While some analysts argue that NATO's global outreach continues to serve a containment logic – counterbalancing other powers' influence in strategic regions – others note that in the Colombian context, the Alliance's footprint seems less about containing a rival power than about containing transnational security threats like narcotics flows or terrorist networks (Sánchez, 2014).

Cooperative security occupies a middle ground. It relies on joint efforts to manage evolving threats and to stabilize fragile contexts through partnership rather than strict alliance obligations (Palma, 2025). Unlike classical alliances, these partnerships are flexible, with no Article 5 guarantee, allowing NATO and partner states to pursue specific interests – cyber defense, counterterrorism, anti-corruption reforms, or maritime interdiction – without binding treaties. Colombia's ties to NATO exemplify how cooperative security can operate in practice. Military training, capacity-building, and institutional integrity initiatives help align Colombia with NATO standards while respecting Colombia's own security agenda (Clavijo Piñeros, 2017). The synergy achieved in areas such as counterterrorism or demining elevates this relationship beyond a static alliance, suggesting that NATO's approach is part of a strategy that merges deterrence, containment (where necessary), and collaborative problem-solving.

- **Relevant International Relations Theories**

Examining NATO's global partnerships through International Relations

theory reveals multiple lenses – namely neoliberal institutionalism, realism and constructivism – that illuminate the drivers and dynamics of cooperation with countries such as Colombia.

Neoliberal institutionalism, exemplified by Keohane's foundational work on international regimes, posits that institutions mitigate anarchy by supplying rules, norms, and frameworks through which states reduce transaction costs, share information, and achieve mutual gains (Keohane, 1984). Applied to NATO's partnership with Colombia, neoliberal institutionalism would underscore how NATO as an institution fosters cooperation by establishing channels for intelligence-sharing and standardized military practices. Colombia's participation in NATO's Building Integrity (BI) Program (McKellips, 2024), for instance, illustrates the neoliberal institutionalist claim that institutions can help states upgrade governance and reduce corruption costs in defense sectors (Clavijo Piñeros, 2017). The transaction costs associated with learning advanced counterterrorism tactics or obtaining technologies for cybersecurity also diminish in the presence of well-structured institutional frameworks. Colombia thus gains from tapping into NATO's resources, while NATO benefits by incorporating Colombia's expertise in countering terrorist networks (Reith, 2024). In this view, neither side necessarily sees the relationship as purely zero-sum; rather, the institution helps them coordinate around shared interests.

Realist and geopolitical perspectives focus on power balances and strategic calculations, contending that states pursue alliances to maximize security in an uncertain international system (Sánchez, 2014). From a realist vantage point, NATO's outreach to Colombia could be interpreted as part of a broader strategy to secure footholds in regions where rival powers – such as Russia or China – are expanding influence (Zuluaga Cometa & Insuasty Rodríguez, 2022). Realists would point to the tensions Colombia faces with neighboring Venezuela, which has forged ties with Russia, to explain why Colombia might find NATO membership beneficial. Closer ties with a powerful alliance could shift regional power balances, giving Colombia both deterrent and bargaining advantages. Hence, from a realist stance, Colombia's interest in NATO is less about intangible norms and more about securing strategic support to balance potential threats or curb adversaries' ambitions (Sánchez, 2014).

Realist frameworks also note that partnership remains short of full alliance, suggesting NATO does not extend Article 5 commitments to Colombia (Helbig & Lasconjarias, 2017). The arrangement might nonetheless enhance NATO's regional awareness and hamper adversarial actors from gaining stronger positions in Latin America. For realists, these are rational calculations of power, whether or not overtly framed in those terms. Colombia's internal security concerns – terrorist groups, narcotic cartels – may be just as important for NATO if they view illicit

networks as potential threats to the Alliance's broader stability. The synergy arises from common interests in containing these threats, a hallmark of realist logic focused on securing strategic advantage.

Constructivism shifts attention toward the role of shared norms, identity, and values in shaping the preferences of states and alliances (Palma, 2025). Constructivists would argue that NATO's global partnerships are not just about material security but also about disseminating democratic norms, transparency, and human rights practices. In the Colombian case, the partnership includes programs aimed at strengthening military ethics, promoting human rights awareness, and fostering institutional integrity within the Armed Forces (McKellips, 2024). By engaging in NATO-led seminars and adopting NATO standards, Colombian officers gradually align with an international community that values democratic civil-military relations. Constructivists would suggest that this alignment changes Colombia's self-perception from a domestically oriented force battling terrorism to a contributor to global security. Over time, the repeated interactions within NATO forums could socialize Colombian defense officials into the Alliance's collective identity, reinforcing compliance with rule-of-law frameworks (Palma, 2025).

Moreover, constructivists might highlight the symbolic resonance of being the first Latin American NATO partner. This symbolism shapes not only Colombia's global image – signaling a break from the region's historical suspicion of external alliances – but also NATO's identity as a flexible, inclusive security organization (Arciniegas & Dos Santos Filho, 2019). Such normative signaling can matter profoundly for legitimation on the international stage, far beyond the immediate security calculations. The institutionalization of this identity-based alignment could explain why some Colombian policymakers see the NATO partnership as recognition of Colombia's democratic and modern military credentials, reinforcing a self-conception that orients the country toward Western security norms.

NATO's collaboration with Colombia embodies an interplay of neoliberal institutionalist cooperation, realist power-balancing, and constructivist norm diffusion. On one level, institutions provide frameworks for practical collaboration that reduce the costs of knowledge transfer, cybersecurity improvement, and training in advanced military tactics. On a second level, realpolitik considerations exist around balancing regional adversaries and extending strategic footholds in a hemisphere historically less aligned with NATO. On a third level, the partnership resonates with shared norms and identity shifts, as Colombia aspires to integrate into what it perceives as a community of democracies with high professional standards in defense.

These theoretical vantage points do not function in isolation. Colombia's desire for external support to consolidate its post-conflict environment aligns

with neoliberal institutionalist logic, but a parallel realist dynamic is at work when it comes to deterring threats at its borders or balancing extra-hemispheric influences. Simultaneously, NATO's emphasis on institutional integrity training and respect for democratic values taps into constructivist processes that socialize Colombian officers into certain normative frameworks. Hence, the NATO-Colombia relationship underscores how international alliances can be driven by multiple overlapping logics. That multiplicity gives the partnership both a strategic dimension - responding to immediate security challenges – and a normative dimension, encouraging Colombia's deeper assimilation into transatlantic defense standards.

Understanding this mix of motivations and processes sets the stage for examining how NATO and Colombia have operationalized their partnership, as well as how these theoretical factors clarify or complicate the relationship's evolution. The subsequent sections will delve into the actual trajectory of NATO-Colombia relations, the specific fields of collaboration (like counterterrorism and institutional reform), and how the critical assessment of this partnership reflects or refutes key tenets of neoliberal institutionalism, realism and constructivism. By mapping these conceptual underpinnings, we gain clarity on how Colombia's integration into NATO's global network can be explained beyond simplistic notions of alliance-building, toward a nuanced appreciation of the multi-theoretical drivers at work.

3. Development of NATO–Colombia Relations

The trajectory of NATO–Colombia relations is rooted in both the evolution of Colombia's domestic security landscape and NATO's broader strategic vision of expanding partnerships beyond the Euro-Atlantic space. In the preceding sections, the theoretical foundations of NATO's global outreach were discussed, highlighting the interplay of institutionalist cooperation, realist power-balancing, and constructivist norm-building. This section now traces how Colombia and NATO progressively moved from initial contacts in the early 2010s to a full-fledged partnership recognized in 2017, examining the main policy milestones, the drivers that propelled the relationship forward, and the key areas of cooperation that currently shape this unique alliance.

A pivotal point for NATO–Colombia engagement came in 2013 with the signing of a Security of Information Accord. Although relatively modest in scope, this agreement marked the first formal step in establishing protocols for sharing classified information between the two parties (Helbig & Lasconjarias, 2017). On the Colombian side, then-President Juan Manuel Santos portrayed it as a breakthrough that could open the way for deeper cooperation on defense and security matters. Yet, it also triggered skepticism among neighboring countries in

Latin America that historically distrusted NATO's presence outside its traditional sphere. Venezuela in particular reacted strongly, claiming that a foreign military alliance could destabilize regional security. Despite such criticisms, the 2013 accord laid the groundwork for Colombia's gradual alignment with NATO standards in intelligence and communications, a process that required establishing protocols for the safeguarding and handling of sensitive data. This initial step, therefore, not only signaled Colombia's interest in internationalizing its defense and learning from NATO best practices but also showed NATO's willingness to engage a Latin American country with significant internal conflict experience (Helbig & Lasconjarias, 2017).

The next major milestone emerged in 2017, when both parties agreed on an Individual Partnership and Cooperation Programme (IPCP). This arrangement formalized a more comprehensive partnership structure, detailing priority areas such as cyber defense, training and education, building integrity, and maritime security (Helbig & Lasconjarias, 2017). By establishing the IPCP, Colombia gained a clearer roadmap for interoperability exercises with NATO forces, officer exchanges, and shared initiatives to uphold transparency in defense administration. On NATO's side, the IPCP validated Colombia's potential contribution in intelligence-gathering, counter-terrorism expertise, and specialized skills in domains such as humanitarian demining. Soon after the IPCP was finalized, the Santos administration presented it as a turning point that elevated Colombia from a mere cooperation partner to a more systematic participant in NATO-led activities. Nonetheless, Colombian officials emphasized that the partnership was not a precursor to NATO membership, given the Alliance's treaty stipulations on geographic eligibility. As a result, the IPCP was understood as a flexible but concrete mechanism for aligning Colombia's evolving defense structures with NATO processes.

Colombia and NATO signed an Individually Tailored Partnership Programme (ITPP) in 2021, which built upon the earlier IPCP by elaborating practical guidelines across a broader range of security issues (McKellips, 2024). The 2021 ITPP introduced specific benchmarks for Colombia's participation in NATO exercises, more advanced joint training in cyber defense, and expanded cooperation on governance standards, often framed under the BI initiative. Through the ITPP, Colombia also reinforced its commitment to institutional reform, seeking NATO's guidance on anti-corruption frameworks and transparent procurement methods for defense equipment. Although each step of Colombia's partnership with NATO emphasized the voluntary and cooperative nature of the relationship – absent the mutual defense obligations that characterize full Alliance membership – each accord incrementally deepened the country's integration into NATO's normative and operational orbit (Rosas Garavito, 2021).

In line with these formal agreements, the year 2017 brought the official designation of Colombia as NATO's first 'Global Partner' in Latin America (Palma, 2025). This label underscored the symbolic importance of Colombia's relationship with the Alliance: for the first time, a South American state was recognized as a participant in NATO's expanding network of global partnerships, which already included Australia, Japan and South Korea. Global Partner status upon Colombia did not imply changes to NATO's collective defense principle or the extension of Article 5 commitments beyond the Euro-Atlantic region. Rather, the designation provided a clearer identity for Colombia's presence in NATO activities and reinforced the sense that Colombia had achieved a threshold of compatibility with NATO doctrines. The Colombian government, meanwhile, interpreted this milestone as an affirmation of the nation's post-conflict transition and a sign that its armed forces were prepared to take on more global security responsibilities (Palma, 2025).

Several drivers stand out in explaining why Colombia and NATO forged such an extensive relationship. First, Colombia's internal context shifted dramatically after the 2016 Peace Accord, which formally ended decades of armed confrontation with the FARC (McKellips, 2024). Although the peace agreement reduced large-scale confrontations, it also created new security challenges such as criminal dissident groups, ongoing coca cultivation, and the delicate process of reintegrating former FARC members. In this environment, in Colombia, there emerged a need for external support to professionalize the Colombian Armed Forces, modernize their doctrines, and enhance governmental oversight over defense spending. NATO, for its part, offered a reservoir of institutional knowledge gained from missions in Afghanistan, the Balkans, and beyond, including experience with post-conflict stabilization, counter-terrorism, and building integrity in military institutions. From Colombia's perspective, partnering with NATO was thus a strategic way of accelerating reforms and positioning the country as a contributor to global security tasks.

Additionally, NATO's own global outreach strategy shaped the partnership's development. Having reaffirmed the concept of 'cooperative security' in its 2010 and 2022 Strategic Concepts, NATO began to extend partnership frameworks to regions outside the alliance's historical area of operations. This outreach was partly motivated by the recognition that security threats—ranging from cyber-attacks to terrorism—often transcend continents (Arciniegas & Dos Santos Filho, 2019). Colombia's proven counter-terrorism expertise, honed over decades of fighting the FARC, ELN, and criminal groups, resonated with NATO's objective of broadening the pool of specialized knowledge within its global partnerships. Indeed, some NATO strategists lauded Colombia's 'lessons learned' in jungle

warfare and intelligence-driven targeting as potentially relevant for international operations that confront irregular militias and terrorist cells (Rosas Garavito, 2021). Thus, beyond symbolic expansion, NATO envisioned Colombia's membership in its global partnership network as a functional gain – one that could enable the Alliance to incorporate new operational tactics and perspectives particularly in counter-terrorism and counter narcotic efforts.

Within this evolving relationship, five key cooperation areas stand out for their relevance and tangible results. The first is training: Colombia's officers have increasingly participated in NATO-sponsored courses (McKellips, 2024). Meanwhile, Colombian military academies have adopted segments of NATO's curricula to enhance English-language proficiency and doctrinal compatibility. The second area is cyber defense. In an age marked by digital vulnerabilities, Colombia has expanded cooperation with NATO to strengthen cybersecurity protocols, focusing on detecting and mitigating cyber threats (NATO, 2024). This collaboration reflects Colombia's concern over hacking attempts from transnational criminal networks, as well as NATO's broader interest in enhancing cyber resilience among its global partners.

A third key area - Building Integrity – intersects closely with Colombia's post-conflict transition. Through NATO's BI program, Colombian officials have participated in self-assessments and peer reviews aimed at reducing corruption within the defense sector (McKellips, 2024). This initiative, as highlighted by Palma (2025), has significantly contributed to promoting higher standards of accountability and transparency within the Colombian military, addressing longstanding challenges related to corruption and ethical conduct. Implementation of these guidelines has included reforms in procurement transparency, ethics training for officers, and the creation of oversight bodies that track defense spending. While critics note that corruption challenges persist, the initiative has promoted higher accountability standards within the Colombian Armed Forces, in accordance with the Peace Accord's broader objectives for reforming state institutions.

The fourth dimension of cooperation involves maritime security. Palma (2025) emphasizes that Colombia's maritime collaboration with NATO, particularly through operations such as *Campaña Orión*, a series of coordinated naval operations designed to curb maritime drug trafficking route, illustrates the practical benefits of cooperation. Likewise, NATO officials have recognized Colombia's willingness to share know-how from *Campaña Orión*.

Finally, counterterrorism lessons learned and experience sharing have emerged as a fifth area of synergy. In 2023, the NATO Center of Excellence – Defence Against Terrorism in Ankara, Türkiye, conducted a workshop with the participation of Colombian officers and international experts, focusing on

Colombia's lessons learned in counterterrorism (COE-DAT, 2023). In 2024, a NATO Science for Peace and Security Advanced Research Workshop (ISSR, n.d.), also held in Türkiye, brought together Colombian, Turkish, and other international academics and practitioners. That workshop explored the impact of illicit economies on terrorism and counter-terrorism, paying particular attention to the Colombian and Turkish cases. These initiatives underscore the Alliance's interest in understanding Colombia's long battle against insurgent and criminal organizations, as well as Colombia's willingness to disseminate practical counter-terrorism insights gleaned from decades of internal conflict. Together, they signal NATO's broader commitment to creating global platforms where partner states can adapt and refine tactics for combating terrorist networks, criminal financing and hybrid threats.

Looking back to the theoretical reflections from earlier sections, the NATO–Colombia story is best understood as a confluence of neoliberal institutionalism (focusing on the institutional frameworks that reduce transaction costs and spread norms), realism (where both parties see strategic gain, be it in balancing against other influences or gaining operational footholds), and constructivism (as shared values around democracy and integrity shape the partnership). The synergy of these factors underpins how Colombia transitioned from purely bilateral defense ties – historically anchored by the United States – to a more multilateral, internationally recognized arrangement that inserts it into NATO's network. In doing so, Colombia aims to bolster its armed forces' professionalism, align with global best practices, and gain a seat at the table of high-profile security dialogues.

4. Counterterrorism, Security Cooperation, and Mutual Contributions

The NATO–Colombia partnership stands as a paradigmatic example of how cooperative security frameworks can yield mutual benefits in counter-terrorism and broader defense collaboration. Colombia, transitioning from decades of internal conflict to a post-conflict scenario, has sought to modernize and professionalize its armed forces, while NATO has welcomed Colombia's specialized counter-terrorism expertise and regional insights into narcotics-driven insecurity. This section examines the ways NATO has contributed to modernizing Colombia's defense institutions, the operational added value Colombia brings to the Alliance, and the primary gains – but also tensions – that shape the evolving security cooperation between these two actors.

- NATO's Role in Modernizing Colombia's Armed Forces

One of the most visible facets of the NATO–Colombia relationship has been the Alliance's contributions to institutional reform within the Colombian Armed Forces. Although Colombia has a long history of security cooperation with the United States and other Western militaries, joining NATO's global partnership framework introduced a more formalized system for adopting Alliance standards (McKellips, 2024). Chief among these initiatives is the BI program, which focuses on reducing corruption risks and strengthening transparency in defense institutions. Historically, corruption and misconduct in Colombian defense procurement have not only eroded public trust in the military but also undermined the efficiency of operations (McKellips, 2024). By participating in the BI program, Colombia undergoes peer reviews and self-assessments that identify vulnerabilities in defense expenditure and propose corrective measures – such as the introduction of competitive bidding processes, stricter auditing, and ethical training for officers. These measures have encouraged more systematic scrutiny of budget execution in the Colombian Ministry of Defense, helping reduce the opportunities for graft at various levels of the procurement chain.

A second pillar of NATO's modernization footprint in Colombia relates to professional military education. Through an expanding network of joint training and exercises, Colombian officers participate in NATO-run courses that address not only operational planning but also civil–military relations, transparency, and humanitarian operations (Sanchez, 2014). The underlying rationale is that an armed forces institution emerging from a decades-long insurgency may benefit from adopting practices honed through NATO's experiences in post-conflict settings like the Balkans and Afghanistan. For instance, many Colombian officers have attended the NATO School in Oberammergau for specialized instruction in leadership, counter-terrorism, and cybersecurity. This engagement has spurred Colombia's own defense academies to update curricula and align with NATO's emphasis on ethics, respect for international humanitarian law, and transparent command structures (McKellips, 2024). The cumulative effect is a gradual institutional realignment, wherein Colombian military doctrines and operational frameworks more closely approximate Alliance standards.

From an administrative perspective, Colombia has also looked to NATO for guidance in implementing the Phased Armaments Programming System (PAPS), a methodology that structures defense procurement over multi-year cycles, balancing immediate operational needs with long-term strategic priorities (Díaz Reina & Fajardo-Toro, 2020). Previously, Colombian defense spending often responded to urgent conflict-related imperatives, with inconsistent planning cycles. By adopting PAPS-oriented processes, Colombia aims to improve cost-efficiency,

transparency, and predictability in acquisitions. This shift not only streamlines supply chains and logistics but also curbs improvised procurement practices that historically generated cost overruns or corruption allegations (McKellips, 2024). Although adapting PAPS to Colombia's local context still confronts hurdles – such as limited budget ceilings, older equipment sets, and legislative frictions – the overall direction signals a sustained push for modernization that aligns with NATO's well-documented planning frameworks.

- Colombia's Added Value to NATO

While NATO's role in professionalizing Colombia's defense sector is evident, Colombia also brings unique expertise that complements the Alliance's broader objectives. In many ways, Colombia's hard-earned experience in counter-terrorism stands out as a core contribution. For decades, the Colombian Armed Forces battled terrorist groups such as the FARC and the ELN, developing specialized tactics in jungle warfare, intelligence-driven targeting of group leaders, and integrating civilian agencies into operational theaters (Arciniegas & Dos Santos Filho, 2019). These lessons resonate with NATO's post–Cold War missions, which frequently involve asymmetrical warfare scenarios. Colombian instructors have therefore participated in NATO-sponsored seminars, explaining how they calibrated offensives against terrorist groups, balanced force with negotiation, and eventually supported demobilization processes. Though every insurgency has its own sociopolitical dynamics, NATO members view Colombia's practical counter-terrorism experiences as transferable insights for complex theatres such as the Sahel or the Middle East. (Arciniegas & Dos Santos Filho, 2019).

A second realm in which Colombia adds tangible value is humanitarian demining. Decades of internal conflict left Colombia among the world's most mine-affected countries, which led to the establishment of specialized demining units and the Colombian International Demining Centre (Centro Internacional de Desminado, CIDES). Since becoming a NATO Global Partner, Colombia has worked closely with the Alliance to exchange techniques and best practices in humanitarian demining. CIDES has hosted training programs and workshops for international personnel, including from NATO members, showcasing Colombia's battlefield-tested expertise in mine clearance. This collaboration exemplifies how Colombia has transitioned from being a heavily mine-contaminated country to becoming a net contributor to global demining efforts. Such engagements reflect NATO's cooperative security approach and demonstrate Colombia's capacity to project stability through niche capabilities in post-conflict recovery (*NATO, 2024*).

Maritime operations offer a further domain of Colombian know-how, especially

in counter-narcotics interdiction. Campaigns like *Campaña Orión* have proven effective at intercepting illegal drug shipments in the Caribbean and Pacific (Rivera Páez, 2022). Colombia's track record in maritime surveillance, littoral patrols, and intelligence integration has gained traction within NATO's broader focus on transnational threats, particularly those financing terrorist networks. Colombian naval officers embedded in NATO exercises, as well as joint maritime drills with Alliance members, strengthen the international capacity to disrupt illicit flows across global shipping routes. For NATO, establishing maritime security partnerships that stretch beyond its traditional perimeter is an increasingly pressing need in an era where non-state actors exploit vast oceanic avenues for contraband and smuggling. Consequently, Colombia's maritime experiences align neatly with Alliance priorities that consider drug-financed terrorism a transnational security challenge.

- Operational Gains and Challenges

Although both sides generally regard the NATO–Colombia partnership as a success, the operational dynamics entail a range of gains and constraints. On the positive side, the partnership has clearly enhanced interoperability. Through repeated exchanges, joint exercises, and officer rotations in NATO-run training schools, Colombia's forces have adopted common tactical language, planning protocols, and command-and-control formats that align with Alliance standards (Díaz Reina & Fajardo-Toro, 2020). This process reduces friction should Colombian units need to work alongside NATO elements in a crisis, whether for humanitarian relief, counterterrorism, or peacekeeping. Observers note that Colombian participation in specific NATO exercises has tested the compatibility of communications systems, rules of engagement, and response procedures (Díaz Reina & Fajardo-Toro, 2020). While Colombian forces, of course, do not have the same integrated command structure as full NATO members, the improved capacity to 'plug in' to NATO-led operations is no small achievement for a Latin American military that was once primarily inward-focused on domestic insurgencies.

A related benefit is the impetus for continued institutional reform. Thanks to consistent engagement with NATO's BI program and PAPS methodology, Colombia's Ministry of Defense has been compelled to adopt more rigorous procurement and financial oversight standards (McKellips, 2024). Corruption in the armed forces, once entrenched, has increasingly become an issue that senior Colombian commanders must address, not only to avoid domestic scandal but also to preserve the credibility of the partnership. Over time, such integrative pressures can lead to a virtuous cycle, in which abiding by NATO's normative frameworks – on ethics, corruption prevention, and accountability – reinforces the Armed Forces' legitimacy in the eyes of the Colombian public. This shift, in turn, indirectly supports the objectives of the

2016 Peace Accord by advancing transparency and state-building.

On a wider scale, another often cited positive consequence is the partnership's impact on Colombia's global diplomatic leverage. Since achieving the status of NATO Global Partner in 2017, Colombia has enjoyed increased prominence in international forums, both within and outside Latin America (Rivera Páez, 2023). While the partnership does not guarantee a seat at NATO decision-making tables, Colombia's officers can join key committees, seminars, and training initiatives that strengthen Colombia's defense diplomacy. Internally, pro-NATO leaders in Bogotá have seized upon this association to frame Colombia as a responsible contributor to global security, in line with the country's ambitions to transcend its legacy of domestic conflict. Externally, certain allies in North America and Europe have welcomed Colombia's involvement in maritime interdiction and humanitarian demining missions, commending it as a sign that Colombia is prepared to help shoulder international security burdens. Even if the scale of Colombian engagement remains modest, the symbolic effect of associating with NATO has lent Colombia an aura of strategic seriousness, helping it garner supportive stances from partners interested in stable security cooperation across the Western Hemisphere.

Yet, the partnership also faces logistical and financial hurdles that may limit the depth of operational integration. For instance, adopting NATO interoperability standards often requires equipment upgrades, improved command infrastructure, and English-language training for a wide segment of the officer corps. Colombia's defense budget, although substantial by regional standards, does not compare to that of the Alliance's major powers. Hence, procuring NATO-compatible communications or advanced defense systems can stress Colombia's resources if not carefully planned over multiple fiscal cycles. The institutional bureaucracy involved in PAPS implementation – where major acquisition programs must be structured over multi-year horizons – sometimes runs up against short-term political priorities in Bogotá. If the impetus for new procurements or infrastructure expansions is overshadowed by immediate demands (e.g., tackling illicit economies, responding to domestic protests or fulfilling social programs), it can slow Colombia's path to deeper interoperability with NATO.

Moreover, tensions persist regarding how Colombia should balance its internal security imperatives against the external engagements encouraged by NATO. Colombia is still grappling with FARC dissident factions, ELN groups in several regions, and emergent criminal organizations. Committing resources to multinational exercises or distant deployments might divert attention from pressing domestic threats, especially in remote rural zones (Sánchez Alemán, 2023). While the Colombian high command stresses that synergy with NATO fosters more robust and adaptable forces, skeptics argue that too strong an alignment with NATO's

external missions could overshadow local security imperatives. This tension manifests in policy debates: for instance, should the Colombian Navy expand its capacities for transatlantic operations in line with NATO frameworks, or remain primarily oriented toward interdiction of drug trafficking near domestic waters? In the medium term, reconciling these competing demands will be a key test of the partnership's sustainability.

Compounding these domestic and regional debates are NATO's own strategic considerations. While the Alliance recognizes Colombia's achievements in counter-terrorism, maritime interdiction, and demining, it must also weigh finite resources and the imperative of addressing immediate threats, such as tensions on its eastern flank in Europe. Expanding cooperation with a non–Euro-Atlantic partner entails some measure of reallocation. The impetus behind global partnerships is to develop flexible security relationships that address shared threats, but NATO's main strategic horizon remains Europe and the North Atlantic, especially in the context of renewed great-power competition. Thus, even if the functional synergy between Colombia and NATO is strong, the partnership may have upper limits on how far operational integration can go, short of membership. As a result, it is more accurate to regard the alliance with Colombia as an evolving, selective cooperation than an all-encompassing security architecture.

In sum, NATO's role in modernizing Colombia's Armed Forces ranges from fostering institutional reforms against corruption to introducing advanced doctrines of interoperability. Colombia's added value to NATO, in turn, stems from its extensive counterterrorism lessons, humanitarian demining proficiency, and proven maritime interdiction capabilities. These mutual gains are, however, tempered by logistical constraints, differing strategic priorities, and political misgivings both within Colombia and across Latin America. The real measure of the partnership's success will be how effectively it navigates these tensions, reconciling Colombia's internal security needs with NATO's global crisis management interests, and ensuring that deepening cooperation neither overextends the Colombian defense budget nor inflames regional diplomatic frictions.

5. Comparative Perspectives

When placed in comparative perspective with other global partners, Colombia's experience reveals both parallels and marked differences. Countries such as Australia, Japan, and South Korea illustrate how global partners can deepen cooperation by contributing forces to NATO-led missions in Afghanistan or through advanced interoperability programs. Those nations share liberal-democratic traditions, possess relatively advanced militaries, and emphasize capacity building in domains like cybersecurity and maritime security. Yet,

none of them has faced the internal insurgencies that have defined Colombia's modern history. Consequently, Colombia brings distinct post-conflict priorities to the relationship, which revolve around upgrading internal governance and reorienting the military for domestic stabilization, even as the country seeks partial integration into transatlantic security initiatives (Helbig & Lasconjarias, 2017). Japan's and South Korea's alliances with the United States, along with their well-funded militaries, allow them to co-develop technologies or host large-scale joint maneuvers with NATO states, while Colombia is comparatively limited by budget constraints and a high domestic security burden.

Australia, for its part, has participated in overseas NATO missions and built substantial interoperability with Alliance forces through combined deployments, arguably more so than Colombia has been able to do. By contrast, Colombia's capital of experiential knowledge lies primarily in counterterrorism, anti-narcotics, and humanitarian demining. Although that expertise has proven relevant to NATO's approach to hybrid and irregular threats, it does not align perfectly with the expeditionary model that states like Australia, deploying alongside the United States, have adopted. Furthermore, Australia's robust economy and advanced defense sector facilitate a sophisticated partnership with NATO that extends to high-technology procurement and intelligence operations. Colombia's defense spending, though significant within Latin America, remains lower and is subject to a volatile political environment (Gómez, 2024).

A final contrast emerges around the factor of post-conflict transitions. Colombia's path to partnership involves reconciling a newly established domestic peace with aspirations for a global security footprint. While states like Japan and South Korea forged or deepened their partnerships in response to external threats or strategic realignments, Colombia's impetus has come at the tail end of an internal war. Therefore, the synergy with NATO must address not only external risk scenarios but also pressing domestic reforms that are core to consolidating peace. The presence of dissident factions and organized criminal networks means that Colombia's defense apparatus continues to focus extensively on internal stability, often overshadowing the possibility of major out-of-area deployments under NATO auspices (Gómez, 2024). This post-conflict reality has shaped a unique blend of cooperation that fuses external capacity-building with domestic institutional transformation, giving Colombia a hybrid role that does not precisely mirror the classical global partners in Asia-Pacific or Oceania.

Taken together, these comparative insights indicate that Colombia does not neatly fit either the profile of a purely geopolitical partner or that of a partner whose role is limited to the transfer of operational know-how. Rather, it occupies a hybrid position: geographically situated in a region where extra-hemispheric competition and U.S.

influence remain salient, yet simultaneously distinguished by its niche expertise in counterterrorism, counter-narcotics, and post-conflict institutional reform. This dual character helps to clarify why NATO treats Colombia differently from partners such as Australia, Japan, or South Korea, whose engagement is primarily framed in terms of high-end interoperability and forward deployment. In Colombia's case, the partnership is driven as much by the diffusion of practices and lessons learned from internal war as by broader calculations about regional balances of power. This boundary-spanning role links the comparative discussion back to the theoretical framework of neoliberal institutionalism, realism, and constructivism, underscoring how Colombia's trajectory blends material, institutional, and normative logics in a way that sets it apart from other global partners.

6. Future Prospects, Policy Recommendations

Although the NATO–Colombia partnership has already yielded tangible benefits in areas such as maritime security, integrity-building reforms, and capacity-building programs, further progress depends on identifying new avenues where both parties can deepen and refine their collaboration. One promising avenue for further collaboration lies in enhancing cyber defense. Colombia, already contending with hacking attempts linked to narcotrafficking networks, stands to benefit from more intensive cooperation with NATO's cyber defense centers. Closer data-sharing, more frequent joint cyber exercises, and expanded best-practice exchanges would fortify Colombian infrastructure against ransomware and espionage, while also advancing NATO's goal of building a broad global coalition that is resilient in the face digital threats. Colombian authorities would need to invest in robust IT systems and specialized personnel, but in return, they would gain from the Alliance's expertise in detecting and mitigating hostile cyber operations. This deeper synergy could better protect Colombia from criminal intrusions and simultaneously enrich NATO's collective awareness of cyber risks emerging from illicit economies.

A second area of growth involves counter-terrorism collaboration and the nexus between terrorism and illicit economies. The extensive Colombian experience with armed groups that merge political or ideological aims with criminal pursuits—especially drug trafficking—offers lessons relevant to many NATO member and partner states confronting hybrid organizations. Workshops held in 2023 and 2024 at the NATO Center of Excellence – Defence Against Terrorism in Ankara (COE-DAT, 2023), as well as the NATO Science for Peace and Security Advanced Research Workshop in Türkiye (ISSR, n.d.), underscored the potential for both Colombia and other Alliance nations to learn from each other's experiences in disrupting the financing of terrorist and insurgent activities. By sharing case studies on dismantling

terrorist structures and curbing narcotics-financed militancy, Colombia contributes valuable models, while also benefiting from fresh perspectives on terrorism in different regional contexts. Strengthening such forums for lessons learned and best-practice sharing could give rise to more integrated, practical approaches to tackling the multifaceted threats that span ideology, crime and global security challenges.

Another prospective step would be a selective expansion of officer placements or secondments, wherein Colombian personnel embed for short stints in NATO's specialized counter-terrorism or cyber units. While the partnership has facilitated general training and seminar attendance, more enduring secondments could accelerate knowledge transfer and allow Colombian officials to adapt state-of-the-art methods for mitigating the nexus of insurgency, terrorism, and transnational criminal financing. This approach would not duplicate the foundational programs already in place but rather build on them by tailoring new projects that specifically address hybrid forms of militancy—an issue drawing increased attention within NATO. Conversely, Colombia's longstanding insights into insurgent revenue streams and criminal infiltration could aid NATO in crafting more flexible responses to evolving threats globally.

Although ongoing maritime cooperation remains beneficial, particularly regarding narcotics interdiction, greater emphasis on these newer, technology-driven and research-focused fields could reassure regional observers that NATO–Colombia ties extend beyond pure defense planning. Framing new initiatives around scientific collaboration and knowledge-sharing may also lessen concerns in neighboring states about foreign deployments or external bases. Colombia thus has an opportunity to cement a reputation as a hub of specialized expertise in counter-hybrid warfare, in turn earning NATO's sustained support for sophisticated innovation ventures. By concentrating on these forward-looking dimensions – cyber resilience, counterterrorism financing studies and structured secondments – NATO and Colombia can refresh the partnership with concrete, future-oriented projects that neither replicate nor dilute existing efforts but instead open pathways for advanced practice and genuine thought leadership in security governance.

7. Conclusion

The NATO–Colombia partnership exemplifies how a post-conflict nation can leverage external alliances for capacity-building while facing the complexities of regional politics and domestic reform. Over the course of incremental agreements, Colombia has sought to improve the efficacy and transparency of its Armed Forces, integrating aspects of NATO doctrine in areas like cyber defense, corruption prevention, humanitarian demining and operational interoperability. NATO, for its

part, has benefited from Colombia's expertise in countering insurgent and criminal groups – knowledge that remains relevant for many of the Alliance's global missions. This reciprocal dynamic underscores how, as contemporary threats proliferate beyond traditional boundaries, alliances evolve into flexible arrangements that merge deterrence, capacity-building, and norm diffusion.

Nevertheless, the future of NATO–Colombia cooperation hinges on the ability of both parties to address residual challenges. Colombia continues to grapple with limited defense budgets and uneven institutional reform Meanwhile, NATO's strategic priorities remain firmly centered on the Euro-Atlantic sphere, complicating how far collaboration with a Latin American partner can progress. These elements reveal the tension between global outreach and local imperatives, a recurring theme in twenty-first-century alliance building.

Beyond these internal and alliance-level constraints, a further external driver that will shape the trajectory of the partnership is the evolving orientation of United States foreign policy toward Latin America in the post-Trump era. As Washington increasingly frames its engagement with the region through the lens of strategic competition with China, South America is likely to acquire renewed prominence in U.S. security thinking, particularly in relation to infrastructure investment, critical supply chains, and maritime routes. In such a context, Colombia's status as NATO's first Latin American global partner may acquire added significance. Colombia's geographic position – connecting the Caribbean, the Andean ridge, and Pacific access routes – renders it an attractive hub, while any intensification of U.S. attention to the region is liable to reinforce, rather than dilute, the incentives for consolidating NATO–Colombia cooperation. At the same time, this renewed focus also reflects a persistent aspiration to preserve a predominant role in the Western Hemisphere, an ambition now articulated less through formal doctrines and more through the contemporary vocabulary of great-power competition with China and Russia.

Still, if recent training activities, research collaborations, and short-term secondments focusing on hybrid threats are any indication, NATO and Colombia appear poised to explore innovative ways of expanding their partnership. Colombia's engagement in advanced research under programs like the Science for Peace and Security initiative suggests that global alliances can thrive on specialized, context-driven projects rather than traditional treaty-bound commitments. As realism suggests, both sides stand to gain strategically; at the same time, neoliberal institutionalism highlights how well-structured programs can reduce transaction costs and deepen trust, and constructivism illuminates how shared norms on governance and ethics reinforce the partnership's legitimacy. Colombia's own trajectory – from a largely inward-focused security apparatus to a state contributing

counterterrorism insights and demining expertise on the global stage – illustrates how alliances can foster significant transformation.

For NATO's broader strategy on global partnerships, the Colombian case thus carries several policy implications. First, it underlines the importance of distinguishing between partners whose main added value lies in geostrategic positioning and those, like Colombia, whose comparative advantage is rooted in specialized know-how, such as counterterrorism, demining and the governance of post-conflict armed forces. Second, it suggests that partnership frameworks should be sufficiently flexible to accommodate hybrid cases where both geography and expertise matter, combining tailored capacity-building packages with selective engagement in regional security dialogues. Third, the experience with Colombia points to the benefits of investing in research-driven initiatives and education programs that institutionalize knowledge transfer rather than relying solely on episodic exercises or symbolic designations. If incorporated into NATO's long-term partnership policy, these lessons could help the Alliance design more differentiated and sustainable cooperation models with other Global South countries that seek to modernize their security sectors while contributing niche capabilities to international stability.

In sum, NATO–Colombia collaboration reflects a shift in how alliances function in a multipolar world. It shows that post-conflict societies can transition from domestic stabilization to global outreach, provided they navigate sovereignty concerns and secure broader political buy-in. For NATO, this case encapsulates how the Alliance diversifies its security network through targeted cooperative frameworks that emphasize training, research, and operational synergies. Looking ahead, balancing Colombia's local imperatives with NATO's overarching strategies will remain a delicate art. Yet, if the partnership continues to yield tangible outcomes, it may well serve as a model for how countries in the Global South, emerging from conflict or facing transnational threats, can tap into alliance-based resources to strengthen their defense sectors while influencing the evolving discourse on global security governance.

References

Arciniegas, A., & Dos Santos Filho, J. E. (2019). Cooperação militar OTAN-Colômbia: Aproximação recente e redefinição do papel das forças armadas colombianas no pós-conflito. *Revista Conjuntura Austral, 10*(49), 13–22.

Clavijo Piñeros, R. A. (2017). *Una explicación del "Acuerdo entre Colombia y la OTAN sobre cooperación y seguridad de información" desde la perspectiva del institucionalismo neoliberal* [Master's thesis] Pontificia Universidad Javeriana.

COE-DAT (Centre of Excellence-Defence Against Terrorism). (2023). *Colombia lessons learned on terrorism workshop report*. https://www.tmmm.tsk.tr/publication/workshop_reports/16-COLOMBIA_LL_ON_TERRORISM_REPORT(2023).pdf

Díaz Reina, J., & Fajardo-Toro, C. H. (2020). Adaptación del sistema PAPS (NATO-Phased Armaments Programming System) en la Armada de Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação, E18*, 458–470.

Gómez, R. D. (2024). Colombia en la OTAN: Implicaciones de seguridad y cooperación internacional. *Revista de la Escuela Superior de Guerra, 38*(2), 45–72.

González Martínez, M. A., Montero Moncada, L. A., Reyes Pulido, Ó. L., & Mejía Rosas, J. L. (2022). Colombia y la OTAN: ¿Una alianza estratégica de disuasión o de contención? *Revista de Relaciones Internacionales, Estrategia y Seguridad, 17*(1), 87–100.

Helbig, R., & Lasconjarias, G. (2017). *Winning peace and exporting stability: Colombia as NATO's next global partner?* (NATO Defense College Research Paper No. 138). NATO Defense College.

ISSR (International Center for Security and Strategy Studies). (n.d.). *Illicit economies and security dynamics: Unveiling insights into conflict, terrorism, and counter-terrorism*. https://ucga.org.tr/index.php/tr/etkinlikler/calistaylar/91-illicit-economies-and-security-dynamics-unveiling-insights-into-conflict-terrorism-and-counter-terrorism-tr

Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.

McKellips, A. I. G. (2024). NATO and the institutional reform of the Colombian armed forces. *Global Policy, 15*(Suppl. 3), 105–119. https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13339

NATO (North Atlantic Treaty Organization). (2010). *Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization: Active engagement, modern defence*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2010/11/19/active-engagement-modern-defence

NATO (North Atlantic Treaty Organization). (2022). *NATO 2022 strategic concept*. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

NATO (North Atlantic Treaty Organization). (2024). *Relations with Colombia*. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-colombia

Palma, O. (2025). Colombia en la OTAN: Cómo se ha convertido un país latinoamericano en socio de la Alianza. *NATO Review*. https://www.nato.int/docu/review/es/articles/2025/01/20/colombia-en-la-otan-como-se-ha-convertido-un-pais-latinoamericano-en-socio-de-la-alianza/index.html

Reith, S. (2024). A security partnership with substance: Colombia as a global partner of NATO. *International Reports* (Konrad-Adenauer-Stiftung), 1/2024, 62–75.

Rivera Páez, S. (2022). Campaña naval y fluvial Orión: Una oportunidad de Colombia para fortalecer la cooperación con la OTAN. *Revista Fuerzas Armadas, 259*, 67–80.

Rivera Páez, S. (2023). *Cumbre de la OTAN en Vilna: Implicaciones geopolíticas y estratégicas para Colombia*. Universidad Militar Nueva Granada.

Rosas Garavito, J. N. (2021). *Los roles de las Fuerzas Militares frente al nuevo papel de Colombia como socio global de la OTAN* [Thesis]. Pontificia Universidad Javeriana.

Sánchez Alemán, Á. P. (2023). *Ingreso de Colombia en la OTAN: Más inconvenientes que beneficios* [Thesis]. Ediciones Universidad Simón Bolívar.

Sánchez, W. A. (2014). Geopolitical considerations of the NATO–Colombia cooperation agreement. *E-International Relations*. https://www.e-ir.info/pdf/47267

Zuluaga Cometa, H. A., & Insuasty Rodríguez, A. (2022). Colombia y la geopolítica de la OTAN: Implicaciones de ser partnership. *Revista Kavilando, 14*(1), 21–27. https://portal.amelica.org/ameli/journal/377/3773733003/html/

Defence Against Terrorism Review

DATR Magazine

Electronic Online ISSN: **1307-9190**

https://dergipark.org.tr/tr/pub/datr

English Article Title (Times New Roman, 14 pt, İtalik, single line)

Name Surname [1,*1] Name Surname [2]

[1]Xxxx Univeristy Xxxx Department,

21Xxxx Univeristy Xxxx Department,

Abstract (must)

"Times New Roman" font should be used in all fields of the article. Line spacing must be "single" in all article fields.

There should be 12 nk space before the title, and 6 nk space after the title. The title should be written in 10 font size, bold, flat and left aligned.

There should be no space before the text (paragraph), and 6 nk space should be left after the text (paragraph). The text should be written in 10 font size, plain and justified.

In this section, a minimum of 100 and a maximum of 400 words in English should be written. In essence, the purpose, scope, research questions of the research should be included, methods, findings and results should be briefly mentioned.

English Keywords: 10 font size, italic. At least 3 keywords must be given. (Times New Roman, 9 pt, single space italic) (Between 200-250)

Keywords

Xxxz, yyyy , ssss, dddd

* The information and views expressed in this article are solely those of the author's and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the author/s is affiliated.

1. Introduction

In this section, the purpose of the research should be specified, then the methods, processes and tools used should be detailed.

The articles should be numbered, including the entry. Subtitles should be numbered hierarchically. The first letter of each word should be capitalized in the titles and subheadings.

The entry title should be written in 11 font size, bold, flat and left aligned. There should be 12 nk space before the entry title and 6 nk space after.

There should be no space before the text (paragraphs), 6 nk space should be left after the text (paragraphs). The text should be written in Times New Roman font, 11 font size, plain and justified.

In the whole article, paragraph heads should be left-justified. Line spacing must be "single" in all article fields.

Page margins should be “Normal” (bottom, top, right, left 2.5 cm).

2. Title

First level titles should be written in 11 font size, flat, bold and left aligned. The first letter of each word must be capitalized. First level should be 12 pt before the title and 6 pt after the title.

There should be no space before the text (paragraphs), 6 nk space should be left after the text (paragraphs). The text should be written in Times New Roman font, 11 font size, plain and justified.

First level title can be used as required.

- **Section headings**

Section headings should be left justified, bold, with the first letter capitalized and numbered consecutively, starting with the Introduction. Sub-section headings should be in capital and lower-case italic letters, numbered 1.1, 1.2, etc, and left justified, with second and subsequent lines indented. All headings should have a minimum of two text lines after them before a page or column break. Ensure the text area is not blank except for the last page.

- **Illustrations**

All figures should be numbered with Arabic numerals (1, 2, 3,….). Every figure should have a caption. All photographs, schemas, graphs and diagrams are to be referred to as figures. Line drawings should

be good quality scans or true electronic output. Low-quality scans are not acceptable. Figures must be embedded into the text and not supplied separately.

3. Tables and Figures

Tables and figures should be included in the relevant text. All tables and figures should be numbered separately. Figure and Table titles should be placed below the figure, aligned in the middle. Figures and tables should indicate the source (according to APA 7 Style).

Tables and figures should be placed in the text as pictures (.jpeg, .png) and also the original formats should be loaded into the system by adding table and figure numbers.

All figures and tables should be cited in the main text as Figure 1, Table 1, etc.

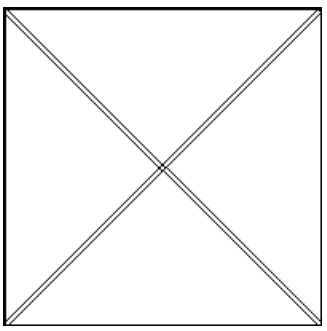
Figure 1. This is a figure. Schemes follow the same formatting.

Table 1. This is a table. Tables should be placed in the main text near to the first time they are cited.

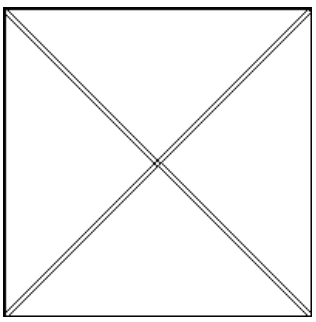
Title 1	**Title 2**	**Title 3**
entry 1	data	data
entry 2	data	data [1]

[1] Tables may have a footer.

The text continues here (Figure 2 and Table 2).



(**a**)



(**b**)

Figure 2. This is a figure. Schemes follow another format. If there are multiple panels, they should be listed as: (**a**) Description of what is contained in the first panel; (**b**) Description of what is contained in the second panel. Figures should be placed in the main text near to the first time they are cited.

Table 2. This is a table. Tables should be placed in the main text near to the first time they are cited.

Title 1	**Title 2**	**Title 3**	**Title 4**
entry 1 *	data	data	data
	data	data	data
	data	data	data
entry 2	data	data	data
	data	data	data
entry 3	data	data	data
	data	data	data
	data	data	data
	data	data	data
entry 4	data	data	data
	data	data	data

4. Conclusions

First level titles should be written in 11 font size, flat, bold and left aligned. The first letter of each word must be capitalized. First level should be 12 pt before the title and 6 pt after the title.

There should be no space before the text (paragraphs), 6 nk space should be left after the text (paragraphs). The text should be written in Times New Roman font, 11 font size, plain and justified.

If necessary, attachments may also be included in the article.

5.Acknowledgments

In this section, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).Acknowledgements and Reference heading should be left justified, bold, with the first letter capitalized but have no numbers. Text below continues as normal.

6. Construction of references

The title of the bibliography should be written in 11 font size, flat, bold and left aligned. The first letter should be capitalized. 12 nk space before the title of the bibliography and 6 nk after the title should be left.

There should be no space before each bibliographic identity given in the bibliography and 6 nk space should be left after the bibliographic identity. The text should be written in Times New Roman font, 11 font size, plain and justified. The second line of the bibliographic identity must be written inside 0.5 cm.

The names of "Journal" and "Book" should be written in italic in the bibliographic identity.

APA 7.0(American Psychological Association) style should be taken into consideration when sending in-text and bibliography. References cited in the text should be listed alphabetically at the end of the study.

Examples:

Aktan, E . (2018). Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu. Bilgi Yönetimi, 1 (1), 1-22.

Al, U., Sezen, U., Soydal, İ., Taşkın, Z. ve Düzyol, G. (2012). Collaboration of Turkish scholars: Local or global? Collnet Journal of Scientometrics and Information Management, 6, 145-159.

Arısoy, Y . (2018). Elektronik Arşivlere Yönelik Uluslararası Yaklaşımlar Çerçevesinde Türkiye Değerlendirmesi. Bilgi Yönetimi, 1 (1), 63-77. Erişim Adresi: http://dergipark.gov.tr/by/issue/37228/415166

Bilgi Mimarisi. (2014, 20 Aralık). Vikipedi İçinde. Erişim Adresi (8 Mayıs 2015): http://tr.wikipedia.org/wiki/Bilgi_mimarisi

Chan, H. F., Guillot, M., Page, L. ve Torgler, B. (2015). The Inner Quality Of An Article: Will Time Tell? Scientometrics, 104, s. 19-41. doi:10.1007/s11192-015-1581-y

EBYS Zirvesi 2016. (2016). Erişim adresi: http://bilbem.ankara.edu.tr/2016/04/21/ebys-zirvesi-2016/

Özdemirci, F. ve Torunlar, M. (2015) Bilgi Çağında Arşivsel Bilgi Analizi: Bilgi-İktidar- İdeoloji-Devlet. Ankara Üniversitesi Basımevi.

"Scan to reach the software of this publication and the other products of COE-DAT"

www.coedat.nato.int