MILITARY ACADEMY

Freelance Terrorism, methods of prevention and combat: A comparative study between Portugal, Poland and France

Aspirant GNR Infantry Diogo dos Santos Almeida

Applied Research Work

Integrated Master's Degree in Military Sciences in the Speciality of Security

Supervisor: Lieutenant-Colonel GNR Infantry (PhD) Tiago Miguel Gonçalves da Silva

Assistant-Supervisor: (PhD) Monika Wysocka

Jury

President of the Jury: Capitan AdMil Daniel Filipe Caiado Durão

External Examiner: Lieutenant-Colonel GNR Nelson Garcia Jacinto

Supervisor: Lieutenant-Colonel GNR Infantry (PhD) Tiago Miguel Gonçalves da Silva

Degree Director: Lieutenant-Colonel GNR Cavalry Lucília de Jesus Mendes da Silva

June 2025

MILITARY ACADEMY

Freelance Terrorism, methods of prevention and combat: A comparative study between Portugal, Poland and France

Aspirant GNR Infantry Diogo dos Santos Almeida

Applied Research Work

Integrated Master's Degree in Military Sciences in the Speciality of Security

Supervisor: Lieutenant-Colonel GNR Infantry (PhD) Tiago Miguel Gonçalves da Silva

Assistant-Supervisor: (PhD) Monika Wysocka

Jury

President of the Jury: Capitan AdMil Daniel Filipe Caiado Durão

External Examiner: Lieutenant-Colonel GNR Nelson Garcia Jacinto

Supervisor: Lieutenant-Colonel GNR Infantry (PhD) Tiago Miguel Gonçalves da Silva

Degree Director: Lieutenant-Colonel GNR Cavalry Lucília de Jesus Mendes da Silva

June 2025

EPÍGRAPH

“If you cry because you’ve lost the sun, the tears won’t let you see the stars!”

Rabindranath Tagore

DEDICATORY

To my sister, my parents, and my comrades from the XXX CFO.

To those who always believed in me, even when the path was uncertain.

"*Ad Astra per Aspera*", without you, none of this would have been possible.

ACKNOWLEDGEMENTS

This applied research is the culmination of five intense and long years of academic study filled with experiences, knowledge, challenges, resilience and lasting friendships. The preparation of this research represents the support of several people, directly or indirectly, who have contributed to the success of this entire journey. In a public, symbolic and sincere way, I would like to express my heartfelt thanks.

To Lieutenant Colonel of Infantry Tiago Silva of the *Guarda Nacional Republicana* (GNR), my supervisor, for his unwavering availability, rigorous guidance, and professionalism. His expertise, commitment and encouragement at every stage were indispensable to the realisation of this dissertation. Thank you for believing in this project as much as I did.

To Dr Monika Wysocka, my co-supervisor, terrorism scholar and a pillar of this research, for her critical insights, generosity, and constant intellectual presence throughout this journey. Despite the physical distance, she was always available to support me with clarity, empathy and commitment. *Z całego serca dziękuję za nieocenione wsparcie, cierpliwość i inspirację. Bez Pani ta praca nie byłaby możliwa*.

To Lieutenant-Colonel of Cavalry Lucília da Silva, Director of the GNR Degrees at the Military Academy, for her readiness to resolve unforeseen difficulties.

To all the interviewees in Poland, who shared their time, professionalism and experience so generously. Their contributions gave depth and credibility to this research. I am also grateful to Radosław Tyślewicz, for the key role played in facilitating this fieldwork and advises.

To all the interviewees, individuals and institutions in Portugal who, when contacted, offered their availability and collaboration in the development of this research, I extend my sincere gratitude. Their contributions, shared to the extent of their time and means, proved truly valuable, enriching the quality and depth of this work.

To my comrades from the *General Adolfo Almeida Barbosa* Course, specifically the XXX GNR Officers' Training Course, thank you for the companionship, solidarity and countless memories throughout these five years. In moments of hardship, you proved what true loyalty and friendship mean. I am grateful to have shared this path with each of you.

A special word of appreciation to my battle buddy and closest comrade, Diogo Salvador. More than a friend, he became a brother. Through encouragement, discipline, and unwavering support, he helped me stand firm through the most difficult moments. For that and more, I am forever thankful.

Last but not least, and in a very special and affectionate way, I would like to thank my family, who believed in me every step of the way, who supported me through the most difficult times and who endeavoured to create the best possible conditions for my journey.

Lastly, and above all, I extend my deepest gratitude to my family and girlfriend. You were the cornerstone of this journey. Your unconditional support and sacrifice gave me the strength to persevere. To my sister Lara, my mother Cristina, and my father Paulo, thank you for always being there, for believing in me and for giving me everything I needed to reach this milestone.

To my grandparents, Helena Quadrado, Anselmo Almeida and Maria Leonilde, who remain present in my life in a special way, I dedicate this achievement with love and respect.

To you, my family, I owe all that I am, as a soldier and, above all, as a man. I carry your name and your values with pride.

Without you it would have been much more difficult.

To you all, my sincere thanks.

Bem hajam!

Diogo Almeida

ABSTRACT

This dissertation examines the phenomenon of Freelance Terrorism and seeks to identify the most effective strategies for its prevention and counteraction in Portugal through a comparative analysis of the institutional and legislative models of Poland and France. Freelance Terrorism is characterised by ideologically motivated acts of violence perpetrated by individual's or autonomous micro-cells, sometimes with formal links to terrorist organisations, which poses a particular challenge to traditional counterterrorism mechanisms. The primary objective was to understand how Portugal can adapt and strengthen its legal and institutional framework in light of the Polish and French experiences.

A qualitative approach was adopted, combining documentary analysis with semi-structured interviews with national and international experts. Due to limited institutional access, the French case was analysed through robust secondary sources. The results show that Portugal operates on a reactive and fragmented model, with legal and operational limitations that prevent effective preventive action. In contrast, Poland follows a more anticipatory model, focused on early detection of behaviour, while France stands out for its centralised and technologically advanced Anti-Terrorist architecture. The research concludes that Portugal should review its legal framework, particularly with regard to the use of metadata and digital surveillance, and invest in institutional and academic cooperation as a way of increasing national resilience against decentralised and asymmetric threats such as freelance terrorism.

Keywords: Terrorism; Freelance Terrorism; Prevention; Combat; Cooperation.

RESUMO

A presente dissertação analisa o fenómeno do Terrorismo Freelance e procura identificar as melhores formas de o prevenir e combater em Portugal, através da comparação com os modelos institucionais e legislativos da Polónia e da França. O Terrorismo Freelance caracteriza-se por atos de violência ideologicamente motivados, perpetrados por indivíduos ou microcélulas autónomas, com algum tipo de ligação formal a organizações terroristas, o que representa um desafio particular para os mecanismos tradicionais de contraterrorismo. O principal objetivo foi compreender como Portugal pode adaptar e reforçar o seu enquadramento jurídico e institucional à luz das experiências polaca e francesa.

Metodologicamente, foi adotada uma abordagem qualitativa, com recurso à análise documental e à realização de entrevistas semiestruturadas com especialistas nacionais e internacionais. Devido ao acesso institucional limitado, o caso francês foi analisado através de fontes secundárias sólidas. Os resultados revelam que Portugal apresenta um modelo reativo e fragmentado, com limitações legais e operacionais para uma ação preventiva eficaz. Em contraste, a Polónia adota um modelo mais antecipatório, com enfase na deteção comportamental precoce, enquanto que a França destaca-se pela sua arquitetura centralizada e tecnologicamente avançada. A investigação conclui que Portugal deve rever o seu quadro legal, nomeadamente quanto ao uso dos metadados e vigilância digital, e apostar na cooperação institucional e académica como forma de reforça a resiliência nacional face a ameaças assimétricas descentralizadas como o caso do Terrorismo Freelance.

Palavras-chave: Terrorismo; Terrorismo Freelance; Prevenção; Combate; Cooperação.

GENERAL CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

INDEX OF APPENDICES

LIST OF ABBREVIATIONS, ACRONYMS AND INITIALISMS

A

ABW	*Agencja Bezpieczeństwa Wewnętrznego* / Internal Security Agency
AM	*Academia Militar* / Military Academy
AF	Armed Forces
AI	Artificial Intelligence
APA	American Psychological Association
Art.º	Article
AW	*Agencja Wywiadu* / Foreign Intelligence Agency

B

BBC	British Broadcasting Corporation
BOA	*Centralny Pododdział Kontrterrorystyczny Policji* / Central Counter-Terrorism Police Unit
BRI	*Brigades de Recherche et d'Intervention* / Research and Intervention Brigades

C

CA	Content Analysis
CDCT	Council of Europe Committee on Counter-Terrorism
CEU	Council of the European Union
CISMIL	*Centro de Informações e Segurança Militares* / Military Intelligence and Security Centre
CPP	*Código de Processo Penal* / Code of Criminal Procedure
CRP	*Constituição da República Portuguesa* / Constitution of the Portuguese Republic
CRQ	Central Research Question
CRS	*Compagnies Républicaines de Sécurité* / Republican Security Companies

D

DCIAP	*Departamento Central de Investigação e Ação Penal* / Central Department of Investigation and Penal Action
DCPJ	*Direction Centrale de la Police Judiciaire* / Central Directorate of Judicial Police
DGSE	*Direction Générale de la Sécurité Extérieure* / General Directorate for External Security
DGSI	*Direction Générale de la Sécurité Intérieure* / General Directorate for Internal Security
DNRED	*Direction Nationale du Renseignement et des Enquêtes Douanières* / National Directorate for Customs Intelligence and Investigations
DRM	*Direction du Renseignement Militaire* / Directorate of Military Intelligence
DRSD	*Direction du Renseignement et de la Sécurité de la Défense* / Directorate for Defence Intelligence and Security

E

ECTC	European Counter-Terrorism Centre
ECTS	European Counter-Terrorism Strategy

EMGFA	*Estado Maior-General das Forças Armadas* / General Staff of the Armed Forces
ENCT	*Estratégia Nacional Contra-Terrorismo* / Portuguese National Counter-Terrorism Strategy
ETA	Euskadi Ta Askatasuna
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation

F

FBI	Federal Bureau of Investigation
Frontex	European Border and Coast Guard Agency
FSPRT	*Fichier de Traitement des Signalements pour la Prévention de la Radicalisation à Caractère Terroriste* / File for Processing Reports for the Prevention of Terrorist Radicalization
FTF	Foreign Terrorist Fighter

G

GIGN	*Groupe d'Intervention de la Gendarmerie Nationale / National Gendarmerie Intervention Group*
GIOE	*Grupo de Intervenção de Operações Especiais* / Special Operations Intervention Group
GN	*Gendarmerie Nationale* / National Gendarmerie
GNR	*Guarda Nacional Republicana* / National Republican Guard
GO	General Objective
GOE	*Grupo de Operações Especiais* / Special Operations Group
GROM	*Grupa Reagowania Operacyjno-Manewrowego* / Operational-Manoeuvring Response Group
GTD	Global Terrorism Database
GTI	Global Terrorism Index

H

HCR-20 v3	Historical Clinical Risk Management 20, version 3
HUMINT	Human Intelligence

I

ICCT	International Centre for Counter-Terrorism
IG	Interview Guide
Interpol	International Criminal Police Organization
IRU	Internet Referral Unit
ISIS	Islamic State
ITCI	Interview; Transcription; Categorisation; Interpretation

L

LOGNR	*Lei Orgânica da Guarda Nacional Republicana* / Organic Law of National Republican Guard
loi SILT	*Loi renforçant la Sécurité Intérieure et la Lutte Contre le Terrorism* / Law strengthening Internal Security and the Fight against Terrorism
LOIC	*Lei de Organização da Investigação Criminal* / Law on the Organization of Criminal Investigation
LOPJ	*Lei Orgânica da Polícia Judiciária* / Organic Law of Criminal Police

	LOPSP	*Lei Orgânica da Polícia de Segurança Pública* / Organic Law of Public Security Police
	LSI	*Lei de Segurança Interna* / Internal Security Law
M		
	ME	Ministry of Economy
	MIA	Ministry of Interior and Administration
	MJ	*Ministério da Justiça* / Ministry of Justice
	MND	Ministry of National Defense
	MP	*Ministério Público* / Public Ministry
	MSM	Main Stream Media
N		
	NATO	North Atlantic Treaty Organisation
	NEP	*Normas de Execução Permanente* / Permanent Execution Standards
	N.º	Number
O		
	OSCE	Organization for Security and Co-operation in Europe
	OSCOT	*Observatório de Segurança, Criminalidade Organizada e Terrorismo* / Observatory of Security, Organized Crime and Terrorism
	OSINT	Open-Source Intelligence
P		
	PJ	*Polícia Judiciária* / Criminal Police
	PM	Prime Ministre
	PN	*Police Nationale* / French National Police
	PNAT	Parquet National Antiterroriste / National Anti-Terrorism Prosecutor's Office
	PP	*Polska Policja* / Polish National Police
	PSP	*Polícia de Segurança Pública* / Portuguese National Police
R		
	RAID	*Recherche, Assistance, Intervention, Dissuasion* / Research, Assistance, Intervention, Dissuasion
	RASI	*Relatório Anual de Segurança Interna* / Annual Report on Internal Security
S		
	SAT	*Section Antiterroriste* / Anti-Terrorist Section
	SDAT	*Sous-Direction Anti-Terroriste* / Anti-Terrorist Sub-Directorate
	SFS	Security Forces and Services
	SG	*Straży Granicznej* / Border Guard
	SGDSN	*Secrétariat Général de la Défense et de la Sécurité Nationale* / General Secretariat for Defense and National Security
	SIED	*Serviço de Informações Estratégicas de Defesa* / Defence and Strategic Intelligence Service
	SIRP	*Sistema de Informações da República Portuguesa* / Portuguese Intelligence System
	SIS	*Serviço de Informações de Segurança* / Internal Security Intelligence Service

	SIVICC	*Sistema Integrado de Vigilância, Comando e Controlo* / Integrated Surveillance, Command and Control System
	SKW	*Służba Kontrwywiadu Wojskowego* / Military Counter Intelligence Service
	SO	Specific Objectives
	SPAP	*Samodzielny Pododdział Antyterrorystyczny Policji* / Independent Anti-Terrorist
	SPOC	Single Point of Contact
	SRGN	*Sections de Recherches de la Gendarmerie Nationale* / Research Sections of the National Gendarmerie
	SSI	*Sistema de Segurança Interna* / Internal Security System
	START	National Consortium for the Study of Terrorism and Responses to Terrorism
	SWW	*Służba Wywiadu Wojskowego* / Military Intelligence Service
T		
	TE-SAT	Terrorism Situation and Trend Report
	TPCE	Terrorism Prevention Centre of Excellence
	TRACFIN	*Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins* / Intelligence Processing and Action Against Illicit Clandestins
	TRAP-18	Terrorist Radicalisation Assessment Protocol 18
U		
	UAF	*Unidade de Ação Fiscal* / Tax Enforcement Unit
	UCAT	*Unidade de Coordenação Antiterrorista* / Counter-Terrorism Coordination Unit
	UCCF	*Unidade de Controlo Costeiro e Fronteiras* / Coastal and Border Control Unit
	UCLAT	*Unité de Coordinations de la Lutte Antiterroriste* / Unit for Coordinating the Fight Against Terrorism
	UDHR	Universal Declaration of Human Rights
	UEP	*Unidade Especial de Polícia* / Special Police Unit
	UI	*Unidade de Intervenção* / Intervention Unit
	UIF	*Unidade de Informação Financeira* / Financial Information Unit
	UN	United Nations
	UNCCT	United Nations Counter-Terrorism Centre
	UNCT	*Unidade Nacional de Contraterrorismo* / National Counter-Terrorism Unit
	UNGA	United Nations General Assembly
	UNOCT	United Nations Office of Counter-Terrorism
	UNODC	United Nations Office on Drugs and Crime
	USA	United States of America
W		
	WS	*Wojska Specjalne* / Special Forces
Z		
	ŻW	*Żandarmeria Wojskowa* / Military Gendarmerie

INTRODUCTION

Terrorism remains a major security challenge in contemporary society, increasingly marked by decentralised threats. One such variant is Freelance Terrorism, characterised by ideologically motivated acts of violence committed by individuals or micro-cells operating autonomously but often inspired or loosely linked to organised terrorist groups (Silva, 2015; Yitzhak, 2013). This typology challenges traditional counterterrorism models and has gained relevance across Europe, notably following attacks in Manchester, Barcelona and Nice.

Since 2015 it's observable a clear increase trend of lone actors[1], who are heavily influenced by the digital propaganda of the Islamic State (ISIS) and other extremist groups. From 2017 onwards, several attacks in Europe were carried out by individuals radicalised online, thereby heightening concerns over lone-actor terrorism. In this heightened context, the need to understand and prevent Freelance Terrorism becomes not only academically pertinent but also operationally urgent.

Although Portugal has not experienced recent terrorist attacks[2], its national threat level was raised in October 2023[3], reflecting broader European concerns, particularly regarding digital radicalisation and returnees from conflict zones (RASI, 2014–2024). This scenario highlights the operational urgency of understanding and preventing Freelance Terrorism. This dissertation explores how Portugal can strengthen its counterterrorism response by analysing the approaches adopted in Poland and France. France is often seen as a benchmark in counterterrorism due to its post-2015 legislative and tactical reforms, including the

[1] Notable examples include the Manchester attack (2017), in which a jihadist inspired by ISIS detonated a bomb at Manchester Arena, killing 22 people (Europol, 2018) and the Barcelona attack in August 2017, where an extremist used a van to run over civilians on Las Ramblas, resulting in 16 fatalities (Europol, 2018). These attacks demonstrated the lethality and unpredictability of freelance terrorists, reinforcing the need to monitor digital radicalisation, as isolated individuals may cause a high number of casualties.

[2] The likelihood of Portugal being affected by terrorist threats has been increasing for two main reasons. Firstly, as European countries with a more extensive history of attacks reinforce their counterterrorism mechanisms, there has been a displacement of the threat towards countries with lower levels of previous incidents, such as Portugal (RASI, 2019). Secondly, some extremist narratives exploit the Islamic past of the Iberian Peninsula, particularly the period during which the southern region of Portugal (formerly al-Gharb, now Algarve) was part of the Islamic Caliphate, as a rhetorical tool, suggesting the need to "restore" these territories to Islamic control, a message that may be used to incite violence. Additionally, Portugal's geographical position has been identified as a risk factor, given that its territory has previously been used as a logistical base for terrorist networks (Silva, 2015, p. 24).

[3] Notably, following the Hamas attack on Israel in October 2023, Portugal officially raised its national terrorist threat level to "significant" (level 3 out of 5), marking a critical shift in internal security posture. This decision reflects not only broader European dynamics, but also increasing security posture. To learn more about this Portuguese terrorist threat level see subchapter 3.1.1.

implementation of the Plan Vigipirate and Operation Sentinelle (SGDSN, 2016), while Poland has invested in research-based prevention, notably through the Terrorism Prevention Centre of Excellence (TPCE).

The central research question, along with the general and specific objectives and corresponding derived questions, were formulated to guide the investigation and ensure analytical coherence, as Quivy & Campenhoudt (2008, p. 32) and Rosado (2017) argue. Their articulation and justification can be consulted in Appendix H, where the full logical framework of the study is presented, being the central research question: **How can Freelance Terrorism be best prevented and countered in Portugal, based on the case studies of Poland and France?**

Moreover, by focusing on a contemporary and under-theorised typology of terrorism, the study contributes to bridging the gap between academic knowledge and operational practice, a need often emphasised in counterterrorism literature (Cortez, 2021). It follows the NEP[4] 522/2.ª/AM[5] guidelines and is divided into two parts: a theoretical framework (definition, radicalisation processes, national mechanisms and comparative analysis), and a methodological framework with presentation and discussion of results. This is followed by the References, prepared in accordance with the 7th edition of the American Psychological Association (APA) style guidelines (using to this effect the Mendeley Reference Manager software), and the Appendices deemed relevant to the investigation (Biblioteca da Faculdade de Economia, 2024).

[4] *Norma de Execução Permanente* (Standing Execution Order).

[5] Approved by His Excellency the Commander of the Military Academy, Major General Lino Loureiro Gonçalves (Academia Militar, 2024)

PART I – THEORETICAL FRAMEWORK

CHAPTER 1: THEORETICAL FRAMEWORK – FREELANCE TERRORISM

1.1. Definition, Characteristics, and History of Terrorism

Although politically motivated violence has existed for centuries, the term "terrorism" emerged during the French Revolution (1789–1799) to describe the repressive tactics employed by revolutionary factions (Lopes, 2019). By the late 19th century, it became associated with anarchist movements that used political assassination as a means to challenge the established order (Leandro, 2004), thereby marking a transition towards terrorism as a systematic strategy of political subversion.

It is essential to distinguish terrorism from common acts of violence. While both can instil fear, terrorism is characterised by its ideological, political, or religious motivations and by its instrumental use of violence as a form of symbolic communication. Unlike conventional crime, terrorist acts aim not only to harm immediate victims but to influence broader audiences, seeking to alter behaviours, perceptions or policy decisions (Schmid, 2021).

A more detailed discussion on the historical evolution of the concept of terrorism, including the distinction between "terror" and "terrorism", is provided in Appendix A.1.

1.2. Challenges in Achieving an International Definition of Terrorism

The definition of terrorism remains one of the most contested issues in both academic and legal domains. As several authors point out, the diversity of motivations, contexts and forms of terrorism makes it difficult to establish a single, universally accepted definition (Faluyi *et al*., 2019; Cortez, 2021). Cultural, political, and economic conditions significantly influence how terrorism is conceptualised, and as a result, definitions tend to reflect the perspective and strategic priorities of the defining body.

Despite various attempts, ranging from the 1937 Convention promoted by the League of Nations to multiple United Nations (UN) resolutions and more recent European Union (EU) directives, no fully consensual definition has been achieved. While most institutional

definitions converge on the idea of violence used to instil fear and advance ideological, political, or religious aims, they diverge in scope, legal implications, and framing.

This plurality of perspectives has complicated the development of coherent international legal frameworks. For an overview of the most relevant international definitions and legal instruments, such as those adopted by the UN, NATO (North Atlantic Treaty Organization), the EU, the GTI (Global Terrorism index) and the FBI (Federal Bureau of Investigation), see Appendix A.2.

1.3. Typologies of Terrorism

Understanding the evolution of terrorism requires a framework capable of capturing its ideological and strategic diversity. One of the most influential models is David C. Rapoport's "Four Waves of Modern Terrorism", which conceptualises terrorism as a phenomenon that develops in successive ideological cycles: the Anarchist Wave, the Anti-Colonial Wave, the New Left Wave, and the Religious Wave (Rapoport, 2013). Each wave reflects changing geopolitical dynamics and motivations over time (see Appendix A.3).

However, this model has not gone unchallenged. Authors like Parker & Sitter (2016) argue that terrorism is better understood through persistent ideological tensions, such as socialism, nationalism, religious extremism, and political exclusivism, rather than as a linear, wave-like cycle. Others, such as Combs & Slann (2007, p. 320) and Esmailzadeh (2023), emphasise the dual nature of terrorism as both warfare and spectacle, aimed at influencing audiences through fear and destruction.

For analytical clarity, this dissertation adopts a simplified typological model based on Europol's most recent classifications: Jihadism, Left-Wing (and Anarchist), Right-Wing, Separatist (and Ethno-Nationalist), and Other Forms (EUROPOL, 2023). These categories are operationally relevant and reflect contemporary terrorist threats across the EU.

Additional typologies, such as those proposed by Ventura & Dias (2015, cited in Cortez, 2021, p. 40-41), are presented in Appendix A.3 to complement the core framework used in this study.

1.4. Jihadist Terrorism

Religious terrorism represents one of the most enduring and ideologically charged forms of violent extremism, with jihadism emerging as its most prominent contemporary expression.

Jihadist terrorism seeks to legitimise violence through radical interpretations of Islamic doctrine, claiming divine justification for political aims (Henne, 2019).

This movement gained strength following the Soviet–Afghan War (1979–1989), particularly with the rise of Al-Qaeda in the 1990s, and evolved into a decentralised structure with the emergence of ISIS in the 2010s (Gartenstein-Ross *et al*., 2016). These organisations aim to establish a global Islamic order and are adept at using digital platforms to radicalise sympathisers across borders (Schmid, 2021; TPCE, 2021).

Contemporary jihadism combines religious dogma with geopolitical grievances and anti-Western narratives, portraying itself as the defender of Islam against both internal and external threats (Silva, 2015). Within this context, new forms of terrorism such as Freelance and Lone Wolf actors have emerged, individuals who operate independently or with minimal support, often radicalised through digital means. Their unpredictability, symbolic impact, and operational invisibility constitute a significant security concern across Europe (Bakker & Graaf, 2010; Schmid, 2021). Further conceptual clarifications and typological distinctions are detailed in Appendix A.4.

CHAPTER 2: "LONE WOLF" TERRORISM VS FREELANCE TERRORISM

2.1. Radicalization

2.1.1. Concept and Complexity of the Radicalisation Process

Radicalisation is a multidimensional and cumulative process through which individuals or groups progressively adopt extremist ideologies and come to regard violence as a legitimate means of achieving their goals. According to the Terrorism Prevention Centre of Excellence (TPCE, 2021), no one is born a terrorist, rather, individuals become radicalised through a combination of personal, social, political, ideological, and contextual factors.

It is important to distinguish radicalisation from the legitimate exercise of freedom of expression, a right enshrined in Art.º 19.º of the Universal Declaration of Human Rights (UDHR)[6]. While strong or dissenting, views are part of democratic societies[7], extremism becomes violent when it promotes or legitimises the use of force to achieve ideological ends. In such cases, terrorism[8] may be perceived as the only viable path to enact change for individuals undergoing radicalisation.

See also Appendix B.1 for and extended overview of radicalisation pathways and contemporary dynamics.

2.1.2. Stages and Models of Evolution

The process of radicalisation does not follow a uniform or linear path, but rather manifests as a dynamic and individualised progression shaped by diverse and often overlapping influences. Although each case is unique, scholars have identified recurrent stages through which individuals may evolve: from the adoption of polarised beliefs, to activism[9], to

[6] As stated in Art.º 19 of the UDHR – "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas though any media and regardless of frontiers" (UN, 2025b).
[7] Activism falls within the scope of this universal right, insofar as it encompasses all activities carried out in an accordance with the UDHR that aim to bring about social and political change (TPCE, 2021).
[8] Terrorism, by contrast, is characterised by the deliberate use of violence against persons or property, with the objective of intimidating or coercing a particular country or group of people into a specific response (TPCE, 2021).
[9] For example, engagement in peaceful actions aimed at promoting political or social change.

ideological extremism[10], and, ultimately, to violent action[11] (TPCE, 2021). This progression is neither fixed nor inevitable, but its volatility makes it difficult to predict and prevent.

Key drivers of this process include a complex interplay of psychological, social, political, ideological, and cultural factors. These are often activated or amplified by specific catalysts such as ideological mentors (radicalisers), group dynamics that foster collective identity and validation, and the strategic use of digital platforms, which facilitate the dissemination of propaganda and recruitment (TPCE, 2021).

Moreover, contemporary forms of radicalisation present new challenges to national and international security. Notably, phenomena such as online radicalisation, youth susceptibility, and the rise of freelance or "lone wolf" actors highlight the evolving and decentralised nature of modern terrorism. These developments call for more nuanced and adaptive counter-radicalisation strategies that preserve fundamental rights while addressing emergent threats.

A detailed account of the underlying factors, catalysts, and emerging trends associated with radicalisation is provided in Appendix B.1.

2.1.3. The Jihadist Radicalisation Model

The jihadist radicalisation process can be conceptualised through a four-stage model developed by Wictorowicz (2005), Silber e Bhatt (2007) e Sagean (2008), (cited in Cortez, 2021). This framework comprises: i) Cognitive Opening, in which vulnerable individuals become receptive to extremist narratives; ii) Religious Seeking, where they reinterpret their identity through a radical Islamist worldview; iii) Identity Alignment, marked by progressive indoctrination and acceptance of violence; and iv) Socialisation, involving full integration into jihadist networks and potential operationalisation.

An additional element of concern is jihadist recruitment, which often targets socially marginalised and criminally predisposed environments, such as prisons and ghettos, rather than civic or academic contexts. This strategy supports what Cortez (2021) describes as the crime-terror nexus, a convergence of criminal and terrorist behaviours that enhances operational effectiveness (see Appendix B.2).

Drawing on the annual TE-SAT reports published by Europol (2014–2024) and complementary academic literature, a non-empirical profile of radicalised jihadists can be

[10] Characterised by uncompromising and rigid views, where the individual adopts increasingly extreme stances on specific issues, thus departing from activism

[11] Which is the practical application of extremism, hence terrorism.

delineated: typically, males aged 16 to 40, often second or third generation Muslims and predominantly from disadvantaged socioeconomic backgrounds (EUROPOL, 2014-2024; Cortez, 2021).

2.1.4. The Influence of the Digital Environment

The reality of the 21st century has brought a radical transformation in the dynamics of radicalisation, largely due to the widespread use of digital technologies. Terrorist organisations have rapidly adapted to this new environment, exploiting the internet, social media platforms, and mainstream media (MSM) to conduct virtually the entire radicalisation process, from recruitment and indoctrination to (virtual) training and operational mobilisation (Cortez, 2021).

Online propaganda has become one of the most powerful weapons in the jihadist arsenal. Groups such as ISIS and Al-Qaeda have developed sophisticated media branches, such as Al-Hayat Media Centre and As-Sahab Foundation, that produce high-quality audiovisual content with emotionally charged messages and religious justifications aimed at global audiences[12] (Gartenstein-Ross *et al*., 2016). These contents are easily disseminated through platforms like Telegram, YouTube, Twitter (now "X"), and even gaming environments or encrypted forums, which serve both as echo chambers and recruitment hubs (TPCE, 2021).

Recent developments in artificial intelligence (AI) and data algorithms have further intensified this challenge. Recommendation systems used by platforms like YouTube or TikTok may inadvertently lead vulnerable individuals down ideological rabbit holes, progressively exposing them to more extreme content. Deepfake technology and manipulated visual content have also enabled the creation of persuasive and immersive propaganda, making it increasingly difficult to distinguish truth from manipulation (Institute for Economics & Peace, 2025a).

In parallel, MSM may unintentionally contribute to the problem. By offering extensive, immediate, and often sensationalist coverage of terrorist incidents, they risk amplifying the "propaganda of the deed" effect, whereby perpetrators gain the visibility and notoriety they seek. This dynamic may encourage so-called copycat actors[13], isolated individuals who emulate previous attacks for ideological, emotional or narcissistic reasons (Schmid, 2021). This migration of radicalisation into the digital sphere presents severe challenges to traditional

[12] They have even made versions of those in specific languages and oriented to specific countries.
[13] This phenomenon, known as copycat crime, refers to the repetition of violent acts inspired by previous terrorist attacks that have received extensive media coverage. The visibility granted by such coverage may, inadvertently, legitimise or even encourage unstable individuals to replicate these behaviours, often in pursuit of emulation or social recognition. (Bakker & Graaf, 2010)

prevention and detection mechanisms. The virtual realm operates beyond state borders and legal jurisdictions, rendering regulatory control and law enforcement interventions much more complex. As noted by Bakker & Graaf (2010), the internet enables low-threshold entry into extremist environments, fostering a sense of community and identity, while shielding users from surveillance and social sanctions.

Given these factors, contemporary counter-terrorism strategies must prioritise the digital front by integrating cybersecurity, artificial intelligence, online counter-narratives, and closer cooperation with private technology companies. Without a multidimensional and internationally coordinated response, digital radicalisation is likely to remain one of the most prolific and elusive threats to public security.

Lastly, it is important to emphasise the growing relevance of individual radicalisation, particularly among young, socially excluded individuals who are often second-generation immigrants and marginalised within their communities (Silva, 2020; Silva, 2015). These individual actors[14], frequently exposed to digital propaganda and lacking strong social ties, may progress toward violent extremism in isolation. This phenomenon will be explored in greater detail in the following chapters, with particular attention to the typologies of Lone Wolf and Freelance Terrorism.

2.2. Prevention

2.2.1. General Framework

In the 21st century, terrorism prevention has become a core element of national and international security policies, given the complexity, volatility, and unpredictability of contemporary threats. Effective prevention strategies must be multidimensional, incorporating educational, behavioural, legislative and operational components (Cortez, 2021).

As Schmid (2021) argues, prevention is not merely about reacting to past events but about anticipating and avoiding potential crises. This requires the adoption of "backward reasoning", meaning a strategic process that aims to avert plausible but undesirable future

[14] The individuals who carry out acts of terrorism have been subject to a range of terminological classifications, each reflecting different analytical frameworks and strategic priorities. In addition to the widely used terms such as Individual Terrorism and Lone-Actor Terrorism, other expressions have emerged, such as Leaderless Resistance and Freelance Terrorism, which although sometimes treated as synonymous, represent distinct forms of political violence that should not be conflated.

scenarios by acting in the present. In this context, preventive criminal investigations and proactive intelligence gathering have become essential pillars of state security (Cortez, 2021).

Moreover, the ability to foresee future risks depends on the systematic analysis of past and ongoing activities, available capabilities, and the broader sociopolitical landscape. According to Olech (2021), there is a direct correlation between a state's security and its political direction, underlining the crucial role of strategic intelligence in identifying and mitigating emerging threats. A more detailed exploration of this strategic rationale can be found in Appendix B.3.

2.2.2. Preventing Radicalisation: The Starting Point

Radicalisation prevention is widely recognised as the most effective axis of contemporary counter-terrorism strategies, especially in the face of increasingly prevalent ideologically and religiously motivated threats. Europol's TE-SAT reports (2014–2024) underscore the emergence of individuals who, although initially not displaying any signs of extremism, undergo progressive or accelerated radicalisation, culminating in their adherence to violent ideologies. This phenomenon is particularly visible in Foreign Terrorist Fighters (FTF) and Home-Grown Terrorists, including Lone Wolves and Freelance Terrorists (Cortez, 2021). As such, preventing radicalisation, especially violent radicalisation, must be prioritised. It requires an all-inclusive and proactive approach capable of addressing ideological narratives and responding to the new challenges posed by digital tools. The main pillars of such prevention strategies are detailed in Appendix B.3.

2.2.3. Tools for Prevention

The prevention of terrorism relies heavily on technical-scientific tools capable of assessing radicalisation risk and identifying early warning signs. Among the most relevant instruments are the TRAP-18 (Terrorist Radicalisation Assessment Protocol) and the HCR-20 v3 (Historical Clinical Risk Management) protocols (Nowopolski *et al*., 2018), which synthesise behavioural, psychopathological, and contextual indicators that may precede violent acts, particularly in cases of individual radicalisation. Nevertheless, both tools present limitations, including restricted access to clinical or legal data and challenges in cross-cultural applicability (Meloy, 2021; Douglas *et al*., 2014).

Beyond clinical tools, community-based strategies, such as community policing and enhanced HUMINT (Human Intelligence) collection, play a vital role in preventing

radicalisation by fostering trust, promoting local resilience, and enabling the detection of behavioural changes in individuals at risk (Silva, 2015; OSCE, 2014). Public awareness and de-radicalisation campaigns further strengthen prevention efforts, particularly when they actively involve civil society and promote citizenship education, such as “Act Early” (United Kingdom) (Action Counters Terrorism, 2025) and “4U!” (Poland) (University of Gdansk, 2024) exemplify good practices in public engagement.

National and European-level initiatives, including those led by institutions such as the TPCE in Poland and the Council of Europe Committee on Counter-Terrorism (CDCT), reflect a growing recognition of the need for integrated, multidisciplinary, and transnational responses. These initiatives combine educational, psychological, and legal tools to address not only the symptoms of radicalisation but also its structural and ideological roots (Wysocka, 2023; TPCE, 2021; CDCT, 2023). At the European level, the EU Strategic Agenda 2023–2027 highlights deradicalisation and reintegration as essential components of the broader counter-terrorism strategy, particularly regarding the return of women and children from conflict zones (CDCT, 2023).

These multidisciplinary programmes, which combine psychological, educational, and social interventions, aim to deconstruct extremist ideologies and facilitate identity reconfiguration. When adequately implemented, such efforts have shown potential in reducing violent recidivism and supporting sustainable reintegration into society. For a detailed breakdown of the tools and practices referenced, see Appendix B.4.

2.2.4. Combating Online Radicalisation

The fight against online radicalisation represents a central axis of the European Union’s counter-terrorism strategy. The ECTC (European Counter-Terrorism Centre) plays a key role through its specialised unit responsible for monitoring, identifying and facilitating the removal of violent content and extremist propaganda from online platforms. A strategic partnership with internet service providers has been established to curtail the use of digital platforms by terrorist groups, particularly in relation to the dissemination of radical ideologies, operational communication, and incitement to violence (Cortez, 2021). However, the online sphere introduces new complexities. In the digital age, access to personal information, ranging from consumer habits to political and religious preferences, has become a dominant paradigm, shaping both radicalisation strategies and counter-measures (Cortez, 2021).

This information-centred environment has blurred the traditional boundary between preparatory acts (e.g., logistical planning, financing) and the commission of terrorist attacks themselves. In this context, the effectiveness of proactive investigations depends not only on the ability to disrupt planned attacks, but also on the capacity to integrate Open-Source and confidential intelligence, some of which may not be admissible in court (Swallow, 2013, p. 378, cited in Cortez, 2021). Therefore, counter-terrorism efforts must continuously adapt their analytical and technological tools, foster inter-institutional cooperation and develop ethically robust intelligence strategies to detect threats before they materialise.

These dynamics, particularly the intersection between digital intelligence, proactive investigation, and the human factor in online radicalisation, are further detailed in Appendix B.4, which provides an integrated overview of tools and strategic approaches in terrorism prevention.

2.3. “Lone Wolf” Terrorism

2.3.1. Conceptual Framework

Lone Wolf terrorism refers to individuals who, driven by ideological, political or religious motives, perpetrate acts of violence independently, without formal ties to terrorist organisations (Campos, 2021). This conceptualisation clearly distinguishes such actors from members of sleeper cells, who act upon command from structured groups (Bakker & Graaf, 2010, p. 2). Some scholars argue that "Lone Wolf" describes not a category of perpetrator, but a tactical modality characterised by operational autonomy and self-direction (Wysocka, 2023).

In Islamist contexts, Lone Wolves are frequently inspired by jihadist narratives, often accessed online, yet remain organisationally unaffiliated (Wysocka, 2023). Kaplan’s (1997) early definition, cited by Campos (2021), described them as individuals, or small groups, who engage in violence against the state without external command or network support. Later definitions, such as that proposed by Burton and Stewart and adopted by the International Centre for Counter-Terrorism (ICCT), emphasise self-activation and ideological affinity without operational links (Bakker & Graaf, 2010).

Their independence poses significant challenges to detection and prevention, rendering Lone Wolf terrorism a particularly elusive and insidious threat. Although overlapping in some operational aspects, this model is conceptually distinct from Freelance Terrorism, a differentiation further explored in subchapter 2.4.

2.3.2. Operational Typology, Autonomy, Motivations and "Typical Profile"

Lone Wolf terrorists operate with a high degree of autonomy, selecting their targets, methods, and timing based on personal judgement rather than directives from organised terrorist networks. Their motivations often stem from deeply personal grievances, feelings of marginalisation, or ideological influences, yet they typically lack formal links to terrorist organisations (Bakker & Graaf, 2010; Pantucci, 2011; Silva, 2020; Yitzhak, 2013).

A consistent behavioural or sociological profile is absent, with actors spanning diverse ideological backgrounds including jihadism, white supremacy and eco-extremism (Spaaij, 2012). As such, their early detection is often hindered by the inability to apply effective predictive models. They are, therefore, frequently described as true "black swans"[15] (Bakker & Graaf, 2010). Despite their operational independence, Lone Wolves are rarely ideologically isolated, since many draw inspiration from extremist propaganda and publish manifestos to legitimise their actions (Yitzhak, 2013).

Academic literature identifies three main subtypes of Lone Wolf actors: fully isolated individuals; those supported by ideological or logistical facilitators; and informal micro-groups lacking hierarchical organisation (Duarte, 2013). These subtypes illustrate that operational autonomy exists along a continuum and may evolve during the radicalisation process (Pantucci, 2011). Because of this autonomy, Lone Wolves evade traditional surveillance mechanisms, leaving behind minimal communication, financial or network traces. Radicalisation frequently occurs in solitude, often via digital means, blending personal frustration, extremist ideologies and a desire for recognition. Notable examples, including Anders Breivik, Omar Mateen, and Mohamed Merah, illustrate the tactical diversity and psychological complexity of these actors

In addition to the motivational and typological aspects already mentioned, the *modus operandi* of these individuals is characterised by significant operational autonomy, using open sources (such as social networks or technical videos) and a lack of contact with formal terrorist networks. This operational invisibility represents one of the biggest challenges for security services, making it difficult to identify threats early on (Bakker & Graaf, 2010; Silva, 2020; Europol, 2023). For a detailed analysis of these mechanisms, see Appendix B.5.

[15] These attacks are rare and unpredictable, but often have a significant impact. For a more detailed analysis of the "black swan" theory, see Appendix C – "Black Swans" Theory.

2.3.3. Prevention and Challenges

The prevention of Lone Wolf terrorism requires context-specific tools and strategies capable of identifying subtle signs of radicalisation and enabling timely intervention. Instruments such as TRAP-18 and HCR-20 v3 offer a behavioural and psychopathological framework for assessing individual risk (Douglas *et al*., 2014; Meloy, 2021), while community-based approaches grounded in HUMINT and proximity policing facilitate early detection through trust-based engagement (OSCE, 2014; TPCE, 2021).

However, such measures must be implemented with caution to avoid the risk of excessive securitisation, stigmatisation of Muslim communities or infringements on fundamental rights (Reinares & García-Calvo, 2013). Effective prevention thus demands a careful balance between security imperatives and the preservation of democratic values. This balance, along with a multidisciplinary approach that integrates educational, psychosocial and communicational responses, is further detailed in Appendix B.5.

2.4. "Freelance Terrorism"

2.4.1. Conceptual Framework

Freelance Terrorism refers to a form of individual terrorism characterised by operational autonomy but underpinned by ideological or logistical links to formal terrorist organisations (Silva, 2020). While Freelance Terrorists act alone, they are often inspired, guided, or indirectly supported by entities such as Al-Qaeda or Daesh, distinguishing them from "Lone Wolves", who operate without any such connection (Wysocka, 2023). This typology is embedded within the strategic decentralisation of jihadist movements, particularly in what scholars identify as the third phase of global jihadism (Duarte, 2013).

Unlike traditional hierarchical models of terrorism, freelance attacks are typically carried out by individuals radicalised within Western societies, often motivated by propaganda and ideological narratives disseminated online. Despite their solitary operational mode, these actors maintain some level of dependence, whether doctrinal, inspirational or material, on transnational networks. As such, Freelance Terrorism occupies a hybrid space between collective organisational strategy and individual execution, complicating both detection and classification (Reinares & García-Calvo, 2013; Duarte, 2013; Yitzhak, 2013). For a conceptual expansion on terms such as "Individual Jihadism" and "Home-Grown Jihadism", as well as a

detailed examination of the strategic logic of decentralised jihadist movements, see Appendix B.6.

2.4.2. Operational Typology, Autonomy, Motivations and "Typical Profile"

Freelance terrorism is defined by an operational model that merges individual autonomy with varying degrees of ideological and logistical dependence on jihadist organisations such as Al-Qaeda or Daesh (Silva, 2020). Three operational subtypes have been identified: actors radicalised through online propaganda without direct contact; individuals who received limited support, such as training or resources; and small autonomous cells ideologically aligned with transnational jihadist objectives (Silva, 2020). While these actors often act alone, their connection to broader ideological structures differentiates them from Lone Wolves.

In terms of *modus operandi*, these individuals tend to resort to low-sophistication yet highly effective methods, including knives, vehicles, and improvised explosives, often inspired by online jihadist propaganda (Silva, 2020; EUROPOL, 2014–2024). Targets are generally symbolic or densely populated locations, like city centres, schools, places of worship or events, with the selection often reflecting not only ideological motives but also personal grievances and contextual relevance. Planning is typically based on OSINT and digital tools, enabling discreet preparation and execution (Spaaij, 2012; Wysocka, 2023). Another recurrent trait is the presence of a "pre-attack communication phase", where perpetrators publish manifestos or videos declaring their motives, which, while not always sufficient for timely prevention, contribute to copycat dynamics and are relevant for post-attack profiling. The blend of operational autonomy and ideological guidance therefore imposes significant challenges for early detection and reinforces the need for nuanced profiling strategies (EUROPOL, 2023b; Silva, 2020).

Their motivations commonly intertwine ideological adherence with personal grievances, including social marginalisation and cultural disaffection (Reinares & García-Calvo, 2013; Wysocka, 2023). Notably, most attacks occur near the perpetrators' place of residence, highlighting a territorially embedded logic of action (Silva, 2020). Although a standardised profile remains elusive, research suggests recurrent characteristics: young males, often second-generation immigrants, facing identity crises, socio-economic exclusion or unresolved psychological conflicts (Yitzhak, 2013; Silva, 2020). These dynamics reinforce the role of jihadist ideology as a vehicle for symbolic revenge and personal validation. For a detailed discussion of typologies, motivations, and radicalisation dynamics, see Appendix B.6.

2.4.4. Prevention and Challenges

Freelance terrorism presents substantial challenges to prevention due to its operational autonomy and the absence of direct organisational ties. Traditional surveillance and intelligence methods are often insufficient, as these actors typically do not engage in coordinated communications or hierarchical planning. Effective prevention thus requires a multidimensional strategy encompassing behavioural risk assessment tools (e.g., TRAP-18, HCR-20 v3), advanced technological measures such as biometric recognition and geoprofiling, and the ethical use of HUMINT in vulnerable communities.

Community-based interventions and psychosocial programmes play a key role in early identification of radicalisation signs, particularly when implemented by trusted local actors. Concurrently, growing threats from digital radicalisation, such as encrypted forums, deepfakes, and AI-driven propaganda, necessitate updated regulatory frameworks and international cooperation. Balancing human rights with security measures remains a central ethical imperative in designing and applying preventive strategies against freelance terrorism.

For a detailed discussion of typologies, motivations, radicalisation dynamics and prevention mechanisms, see Appendix B.6.

CHAPTER 3 – TERRORISM IN PORTUGAL, POLAND AND FRANCE: COMPARATIVE CONTEXTS

Although the terrorist threat in Portugal is significantly lower than that observed in France, and to a lesser extent in Poland, this does not preclude the ongoing need to strengthen prevention, surveillance, and response measures against emerging threats. The evolution of international terrorism, its transnational character, and its increasingly decentralised nature make it imperative to undertake a comparative assessment of counter-terrorism mechanisms, not only to understand vulnerabilities, but more importantly, to identify best practices that can be adapted to the national context. France and Poland constitute two relevant case studies in this regard, both due to their accumulated experience in facing threats and their legislative and operational choices in countering terrorism.

A quantitative analysis of the terrorist phenomenon, based on data from the GTD[16], reveals that between 2000 and 2020, a total of 139.872 terrorist incidents occurred worldwide, 8.086 of which took place in Europe (START, 2025). Between 2014 and 2020, there were 84.341 global incidents, with 3.878 in Europe. Of these, Portugal recorded only 1 incident, Poland 6, and France 177[17].

Complementing this analysis, the 2025 GTI, which assesses the impact of terrorism across 163 countries, ranks Portugal 100th, Poland 47th, and France 4th, a reflection not only of the number of attacks, but also of their social, economic, and security consequences (Institute for Economics & Peace, 2025b). It is also noteworthy that, according to this report, the impact of terrorism in Europe worsened in 2024, with 25 deaths resulting from 67 terrorist incidents, nearly double the number recorded in the previous year. Most of these attacks were claimed by ISIS and Hamas, and it is particularly concerning that they were planned by lone actors, targeting high-profile events such as the Summer Olympic Games and concerts by artist Taylor Swift, which were foiled by authorities prior to execution (Institute for Economics & Peace, 2025b).

[16] The GTD does not consider planning, reconnaissance, or the acquisition of materials for the execution of attacks as terrorist incidents; it only includes acts officially recorded by states as completed or foiled close to execution.

[17] These data clearly highlight France as one of the most affected European countries during the period under consideration.

Beyond executed or foiled attacks, the TE-SAT reports[18] by EUROPOL (2014-2024) provide essential data on institutional responses to terrorism in EU Member States, particularly regarding arrests, trials, and convictions for terrorist activities. Over this ten-year period, Portugal conducted a total of 9 arrests, including 6 related to jihadist affiliation, 2 for separatist terrorism, and 1 for left-wing extremism. Poland recorded 59 arrests, of which 22 were related to jihadist affiliation and 31 to far-right extremism, indicating a more diverse range of threats. France, on the other hand, conducted 2.742 arrests, including a remarkable 2.335 related to jihadist terrorism, a figure that underscores the country's central role in confronting this particular threat.

These quantitative data highlight not only differences in the degree of exposure and vulnerability among the countries analysed, but also reflect the varying capacities for response, investment in internal security, and the legislative frameworks in force. As will be seen in the following subchapters, prevention and repression strategies in each of the three states are shaped by distinct historical, legal, and geopolitical contexts, which makes it essential to analyse them individually before proceeding to a comparative overview. One crucial consideration in assessing prevention and counter-terrorism strategies is that global cooperation is most effective when it is grounded in consistent national-level counter-terrorism frameworks (Olech, 2021). For detailed data on arrests, attacks, court cases and group affiliations in Portugal, Poland and France between 2013 and 2023, see Appendix E.

3.1. Mechanisms in Portugal[19]

In comparative terms, Portugal presents one of the lowest levels of terrorist incidence within the European Union, a trend that has remained stable over recent decades. According to GTD data, only one terrorist incident was recorded on national territory between 2014 and 2020. This involved a non-lethal attack against infrastructure in 2020, carried out by a single perpetrator (START, 2025). his reality places the country in a position of relative internal stability. However, such stability should not be interpreted as a complete absence of risk, but rather as an opportunity to further strengthen preventive mechanisms.

[18] The TE-SAT reports consider terrorist incidents to include planning, reconnaissance, and the acquisition of materials intended for attacks, as well as all acts recorded by states as completed, failed, or foiled (unlike the GTD).
[19] For detailed data on arrests, attacks, court cases and group affiliations in Portugal, Poland and France between 2013 and 2023, see Appendix E.

Complementing these figures, Europol's TE-SAT reports (2014–2024) record a total of 9 arrests in Portugal for terrorist-related activities. The majority (6) were related to jihadist terrorism, with the remaining cases linked to separatist motivations (2) and left-wing extremism (1). Over the same period, 7 jihadist-related cases were brought to court, resulting in 5 convictions and 2 acquittals, reflecting a relatively high conviction rate of 71%.

Between 2014 and 2020, data extracted from the GTD and analysed through Microsoft Power BI visualization tools, confirms a single terrorist event in Portugal, classified as a facility/infrastructure attack. This attack did not result in fatalities or injuries and had a 0% success rate, highlighting both the low frequency and the limited operational impact of terrorist actions on Portuguese soil during this period. The attack type contrasts with the broader European trend, where armed assaults and bombings are more prevalent (EUROPOL, 2014-2024). Furthermore, no use of firearms, explosives, or mass-casualty techniques was registered in the Portuguese context, further reinforcing the notion of low-intensity and isolated acts. This sole referred case was carried out by a lone actor of unknown affiliation, and did not involve group coordination, complex planning, or critical infrastructure disruption, reinforcing Portugal's profile as a country exposed to minimal terrorist operational activity.

Although limited in number, these data indicate the existence of effective police and judicial interventions aimed at suppressing potential threats. The low number of actualised attacks, combined with a higher number of arrests and trials, may suggest a preventive and proactive strategy on the part of national authorities, in line with the principle of operational anticipation set out in EU directives.

3.1.1. Institutional Response

Portugal's institutional counter-terrorism framework is characterised by a centralised and hierarchical structure that ensures coordination across strategic, operational and tactical levels. Intelligence and political decision-making support are provided by the *Sistema de Informações da República Portuguesa* (Portuguese Intelligence System – **SIRP**) (SIRP, 2025), under the supervision of the *Primeiro-Ministro* (Prime Minister – **MP**), as regulated by Law n.º 9/2007 (Lei n.º 9/2007, de 19 de fevereiro, 2007). SIRP oversees two core intelligence services: the *Serviço de Informações de Segurança* (Internal Security Intelligence Service – **SIS**), focused on internal threats such as terrorism[20] (SIS, 2024), and the *Serviço de Informações*

[20] As per Art.º 3.º n.º 3 and Art.º 10.º n.º 4 of Lei n.º 9/2007, and Art.º 21.º of Law n.º 30/84 (Lei n.º 30/84, de 5 de setembro, 1984).

Estratégicas de Defesa (Defence and Strategic Intelligence Service – **SIED**), dedicated to foreign intelligence (SIED, 2025).

The *Ministério da Defesa Nacional* (Ministry of National Defence – **MND**) contributes through the *Centro de Informações e Segurança Militares* (Military Intelligence and Security Centre – **CISMIL**), responsible for military intelligence, particularly in international missions (EMGFA, 2025). Although the Armed Forces are not primarily responsible for domestic counter-terrorism, they play a supporting role in cyberdefence and crisis management (Campos, 2021; Costa, 2016; Godinho & Pereira, 2019).

Operational counter-terrorism efforts fall mainly under the *Ministério da Administração Interna* (Ministry of Interior and Administration – **MIA**). The *Guarda Nacional Republicana* (National Republican Guard – **GNR**) deploys specialised units such as the *Grupo de Intervenção de Operações Especiais* (Special Operations Intervention Group – **GIOE**) for tactical interventions, alongside units addressing terrorism financing and border control (GNR, 2025)[21]. The *Polícia de Segurança Pública* (Public Security Police – **PSP**) operates the *Grupo de Operações Especiais* (Special Operations Group – **GOE**), with rapid response capabilities for high-risk situations (PSP, 2025)[22].

Criminal investigations, within the *Ministério da* Justiça (Ministry of Justice – **MJ**) are led by the *Polícia Judiciária* (Criminal Police – **PJ**), specifically through its *Unidade Nacional de Contraterrorismo* (National Counter-Terrorism Unit – **UNCT**) and *Unidade de Informação Financeira* (Financial Information Unit – **UIF**), focusing on terrorism financing and cyberterrorism (PJ, 2025)[23].

Strategic coordination is assured by the *Unidade de Coordenação Antiterrorista* (Counter-Terrorism Coordination Unit – **UCAT**), integrated within the *Sistema de Segurança Interna* (Internal Security System – **SSI**). UCAT facilitates inter-agency cooperation and oversees the implementation of the *Estratégia Nacional Contra-Terrorismo* (National Counter-Terrorism Strategy – **ENCT**), while providing threat assessments and supporting political decision-making, as established by the Counsil of Ministers Resolution n.º 40/2023 (Resolução Do Conselho de Ministros n.º 40/2023, de 03 de Maio, 2023). It ensures effective information

[21] As per Art.º 22.º, 40.º, 41.º and 44.º of Organic Law of GNR (LOGNR) (Lei n.º 63/2007, de 6 de novembro, 2007) and Law n.º 83/2017 (Lei n.º 83/2017, de 18 de agosto, 2017) - Preventive and Repressive Measures to Combat Money Laundering and the Financing of Terrorism.

[22] As per Art.º 40.º, Art.º 41.º n.º 1 al. b) and Art.º 43.º of Organic Law of PSP (LOPSP) (Lei n.º 53/2007, de 31 de agosto, 2007).

[23] As per Art.º 4.º n.º 4, Art.º27.º and Art.º30.º of Organic Law of PJ (LOPJ) (Decreto-Lei n.º 275-A/2000, de 9 de setembro), and Art.º 7.º n.º 2 al. l) of Law n.º 49/2008 (Lei n.º 49/2008, de 27 de agosto) (Law on the Organisation of Criminal Investigation - LOIC).

sharing and operational alignment among the various intelligence and law enforcement agencies of the SSI, there represented.

At the judicial level, the *Departamento Central de Investigação e Ação Penal* (Central Department of Investigation and Penal Action – **DCIAP**), within the *Ministério Público* (Public Ministry – **MP**), holds nationwide competence for terrorism cases, overseeing complex investigations and authorising special investigative measures (MP, 2025), in line with Art.º 2.º of LOIC. For a systematised overview of Portugal's counter-terrorism framework, including the key entities, their competencies and legal mandates, see Appendix D.1.

3.1.2. Legislative Framework

Portugal's legislative framework for counter-terrorism has evolved significantly since the 1980s, with early milestones such as the creation of SIRP in 1984 (*Lei n.º 9/2007, de 19 de fevereiro*). The European Union's Action Plan to Combat Terrorism (European Council, 2004) also influenced national legislation by encouraging closer judicial and police cooperation.

The Internal Security Law (LSI) (*Lei n.º 53/2008, de 29 de agosto*)[24] and the Code of Criminal Procedure (CPP) (Decreto Lei n.º 78/1987 de 17 de fevereiro)[25] and LOIC[26] establish strategic, principals, concepts, duties to investigate whether a criminal offence was committed and procedural principles for internal security and criminal investigations (where terrorism falls under). According to Art.º 1.º n.º 1 and 3 of LSI, internal security refers to the activities carried out by the State to ensure public order, safety, and tranquillity, to protect individuals and property, to prevent and suppress crime and to uphold the rule of law and the normal functioning of democratic institutions.

The most significant legislative development came with the adoption of the Law on Terrorism (Lei n.º 52/2003, de 22 de agosto), enacted in compliance with Council Framework Decision 2002/475/JHA and subsequently amended to align with Directive (EU) 2017/541. Although the law does not provide a standalone definition of terrorism, it defines a terrorist group as "an association of two or more persons that (...) is sustained over time and acts in concert with the aim of committing terrorist offences" (Art.º 2.º n.º 1), and characterises terrorist acts as any intentional act already criminalised under Portuguese law that aims to affect national integrity, obstruct public authorities, or intimidate the general population (Art.º 2.º n.º 3).

[24] See Art.º 1.º n.º 1 and 3 of LSI.
[25] See Art.º 262.º n.º 1 of CPP.
[26] See Art.º 1.º of LOIC.

The penal framework imposes prison sentences ranging from 8 to 15 years for participation in terrorist organisations, extending to 20 years for leadership roles, and between 1 and 8 years for preparatory acts. Additional offences such as recruitment, training, travel for terrorist purposes, and financing of terrorism are also criminalised, the latter punishable even without proof of actual use of funds for terrorist acts (Art.º 3.º n.º 1 and 2, Art.º 4.º n.º 1, and others of Lei n.º 52/2003).

Portugal's ENCT and the UCAT are grounded in LSI and the Council of Ministers Resolution n.º 7-A/2015 (Resolução do Conselho de Ministros n.º 7-A/2015), providing for strategic coordination and operational response within internal security[27,28], later updater by Resolução do Conselho de Ministros n.º 40/2023, de 03 de Maio (2023)[29].

Nevertheless, several scholars have highlighted limitations in the legal framework, particularly concerning preventive investigative measures. Silva (2015) critiques the legal constraints on preventive vehicle searches, suggesting that they should be allowed even without reasonable suspicion, provided they are subject to subsequent judicial validation. Similarly, the regime governing communications interception, currently admissible only at the inquiry phase and requiring prior judicial authorisation (Art.º 187 of the CPP), has been criticised for hampering timely preventive action. Silva (2015) proposes empowering senior criminal police authorities to authorise such measures, with judicial review within 48 hours.

Further proposals include the development of a specialised branch of criminal law, introducing expedited and effective substantive and procedural instruments. Examples include criminalising the glorification of terrorism and self-radicalisation, enhancing penalties for terrorist financing even without proof of use and expanding the admissibility of undercover operations and metadata collection without prior judicial authorisation. It is also important to propose adjustments to enhance operational effectiveness while safeguarding fundamental rights guaranteed by the Constitution of the Portuguese Republic (CRP, 1976), such as the presumption of innocence (Art.º 30.º n.º 2 CRP) and the prohibition of torture (Art.º 25.º n.º 2 CRP) (Rui Pereira, cited in Silva, 2015).

---

[27] As per Art.º 1.º n.º 1 of LSI, internal security is defined as "the activity carried out by the State to ensure public order, safety and tranquillity, to protect individuals and property, to prevent and suppress crime, and to help ensure the normal functioning of democratic institution".

[28] As per Art.º 23.º of LSI and Art.º 2.º of Regulatory Decree n.º 2/2016 (Decreto Regulamentar n.º 2/2016, de 23 de Agosto, 2016).

[29] This reflects a commitment to the "mobilisation, coordination, and cooperation of all national structures with direct and indirect responsibility in combating the terrorist threat," and represents a concrete national-level implementation of internal, European and international counter-terrorism imperatives (Resolução do Conselho de Ministros n.º 40/2023, de 03 de maio).

Finally, in situations of imminent terrorist threat, fundamental rights may be temporarily suspended under a state of emergency or siege, with operational command falling under SSI as per Art.º 8.º, Art.º 9.º and Art.º 19.º of LSI. For a systematised overview of Portugal's counter-terrorism framework, including the key entities, their competencies and legal mandates, see Appendix D.1.

3.1.3. *Estratégia Nacional de Combate ao Terrorismo* (ENCT)

The ENCT is closely aligned with the European Counter-Terrorism Strategy (ECTS), reflecting the same structural framework based on four fundamental pillars: prevent, protect, pursue and respond (*Resolução do Conselho de Ministros n.º 40/2023, de 03 de maio*). This convergence underscores Portugal's commitment to the European values of security, peace and stability, while assuming an active role in the neutralisation of terrorist threats and violent extremism (*Resolução do Conselho de Ministros n.º 40/2023, de 03 de maio*).

The Prevent pillar focuses on addressing the root causes of radicalisation, particularly targeting youth and countering online extremist propaganda. The strategy also prioritises the development of a National Action Plan[30] aimed at preventing radicalisation and terrorist recruitment. Particular emphasis is placed on combating disinformation and hate speech online, controlling access to weapons and hazardous substances, preventing money laundering and terrorist financing. Protect aims at enhancing the resilience of critical infrastructure and public spaces through strengthened cooperation among intelligence services, law enforcement, and judicial authorities, along with improved cybersecurity and border control. Under Pursue, efforts concentrate on disrupting terrorist networks and financing structures, ensuring respect for human rights and adapting legislation to the evolving nature of terrorism. This pillar also aims to improve coordination between entities involved in the identification and referral of individuals with mental health disorders who may be potentially linked to terrorist behaviours. Finally, Respond focuses on the management, preparedness and mitigation of potential consequences arising from a terrorist attack that has already been carried out. It also encompasses the coordination between the AF and SFS, as well as the protection of victims of terrorism, ensuring their recognition as particularly vulnerable victims and the upholding of their rights. Compared to the previous version, the former pillar "Detect" has been integrated

[30] As per Art.º 1.º Point II al. i) of Resolução Do Conselho de Ministros n.º 40/2023, de 03 de maio.

into the current structure, particularly under the Prevent and Pursue domains, reflecting the emphasis on early identification of radicalisation, isolated actors and the use of technology.

However, significant legal limitations persist in Portugal regarding electronic surveillance and interceptions[31] outside criminal proceedings, particularly impacting the early detection of threats by intelligence services. In part, it happens because these act at the "pre-active" stage, directly involved in the detection of threats through information gathering. At this point, no offence has yet occurred or materialised, meaning no criminal proceedings have been initiated. As a result, the national legal framework does not permit this essential measure, electronic interception, at this stage. Even though there is an exception legally provided for, it is only applicable during the inquiry phase, which presupposes the prior initiation of criminal proceedings. This creates a legal obstacle for intelligence services in carrying out a measure that is deemed crucial for the detection of terrorist threats on national territory, particularly in relation to Freelance Terrorism[32]. Under the current legal framework, intelligence services are only authorised to access metadata[33] associated with a given telephone device. This, however, is insufficient, as they also require access to the content of communications

3.2. Mechanisms of Poland[34]

Poland is regarded by European authorities as a territory of increasing potential risk, despite having a low rate of actualised terrorist incidents and being commonly used as a transit corridor. This perception stems from several factors: Poland's membership in both NATO and the EU, its strategic location on the eastern flank, and its geographical proximity to zones of instability, such as Ukraine[35]. Another reason why Poland may be characterised as a potential target for terrorist attacks lies in its active participation in international operations in territories

[31] The legal framework relating to this matter is set out in Art.º 34.º, n.º 4 of CRP, which states: "All interference by public authorities in correspondence, telecommunications and other means of communication is prohibited, except in cases provided for by law in matters of criminal procedure.". These exceptions are detailed in Art.º 187.º n.º 2 al. a) of CPP.

[32] In the case of Freelance Terrorists, two distinct typologies may be observed. If an individual is found to be planning an attack using improvised explosive devices and there is evidence that such devices are being stored at their residence, the legal framework allows for electronic interceptions to be authorised. However, if an attack is planned using a vehicle as a weapon, as was the case in the Nice attack in France and the Barcelona attack on *Las Ramblas* (a *modus operandi* identified as widely used according to TE-SAT 2014–2024), there is no legal basis for authorising such interceptions, as a vehicle is not inherently classified as a weapon and its possession is legal.

[33] In other words, authorities may be able to access metadata regarding an individual's communications, but not the content of those communications.

[34] For detailed data on arrests, attacks, court cases and group affiliations in Portugal, Poland and France between 2013 and 2023, see Appendix E.

[35] Where an ongoing conflict with Russia persists.

controlled by terrorist groups, its involvement in global counter-terrorism efforts, internal political disputes and its ongoing cooperation with the USA[36] (Olech, 2021). This strategic context justifies the adoption of a robust prevention strategy, focused on threat anticipation and the deterrence of extremist activity (Olech, 2021, Olech, 2022a). Accordingly, Poland seeks to eliminate emerging threats through its specialised entities, thereby preventing the occurrence of terrorist attacks or the escalation of their potential risk (Olech, 2021).

According to GTD data, Poland recorded only six terrorist incidents between 2014 and 2020, none of which resulted in fatalities or significant damage (START, 2025). However, the TE-SAT reports (2014–2024) reveal a notable total of 58 arrests related to terrorist activities. Of these, 31 were linked to right-wing extremism, 22 to jihadist terrorism, and the remaining 5 to other forms of terrorist affiliation. During the same period, four jihadism-related cases were tried in court, resulting in three convictions and one acquittal, reflecting a relatively high conviction rate of 75%.

Between 2014 and 2020, the GTD confirms a total of six terrorist incidents in Poland, all of which were classified as bombing/explosion attacks, a method commonly associated with anarchist or extremist protest actions. These incidents resulted in no fatalities or injuries, and the overall operational success rate was 83%, indicating that while the attacks did not cause human casualties, they were executed according to plan or intended disruption. Compared to the European average, this reflects a low-impact but non-negligible threat landscape, with attacks targeting symbolic or infrastructure-related objectives rather than mass civilian harm. The GTD data analysed via Power BI also reveals that all attacks were of low complexity, not involving firearms, hostage-taking, or coordinated assault strategies. These patterns reinforce the notion of limited lethality and a tendency towards ideologically-driven symbolic violence. Notably, the absence of armed assaults or high-casualty events differentiates the Polish context from higher-risk environments such as France, and underscores Poland's positioning within the spectrum of low-frequency but ideologically diverse terrorist activity.

3.2.1. Institutional Response

Poland's counter-terrorism framework is structured around three fundamental pillars: specific legislation with broad competences; specialised intelligence and operational agencies;

[36] Considered one of the main enemies of terrorist organisations due to its Global War on Terrorism, the USA has nonetheless seen its image as a counter-terrorism superpower weakened following its withdrawal from Afghanistan (Olech, 2022a).

and robust international cooperation. This structure aligns with the European Union's Counter-Terrorism Action Plans, reinforcing efforts in radicalisation prevention, border control, and disruption of illicit financing networks (Wiśniewski, 2018; Wysocka, 2023; Committee of Ministers, 2018).

At the strategic level, the internal security is ensured, under MIA, by the *Agencja Bezpieczeństwa Wewnętrznego* (Internal Security Agency – **ABW**), combining intelligence and judicial police powers[37], and the *Agencja Wywiadu* (Foreign Intelligence Agency – **AW**), focusing on external threats[38] and in identifying and analysing international terrorism and transnational organised crime networks (ABW, 2025; Kochańczyk, 2020; Zięba, 2015). Military intelligence, under MND, is guaranteed by the *Służba Wywiadu Wojskowego* (Military Intelligence Service – **SWW**), focused on external military threats, including terrorism in armed conflict zones (SWW, 2025), and the *Służba Kontrwywiadu Wojskowego* (Military Counterintelligence Service – **SKW**), that ensures internal security within the AF and addresses terrorist threats among military personnel (SWW, 2025; SKW, 2025). These agencies are overseen by their respective ministries but are centrally coordinated by the Minister Coordinator for Special Services (Chancellery of the Prime Minister of the Republic of Poland, 2025).

At the operational and tactical level, the *Polska Policja* (Polish National Police – **PP**) carries out counter-terrorism interventions through specialised units (PP, 2025) such as the *Samodzielny Pododdział Antyterrorystyczny Policji* (**SPAP**), conducts regional anti-terror operations and the *Centralny Pododdział Kontrterrorystyczny Policji* (**BOA**), an elite tactical unit in high-risk and crisis situations, and also functions as a criminal police unit (Zubrzycki, 2017), recognised under Council Decision 2008/617/JHA of 23 June 2008; PP, 2025a). Border security operations are managed by the *Straż Graniczna* (Border Guard – **SG**), equipped with reconnaissance and preventive capacities (Puacz-Olszewska, 2019)[39].

Military support is provided by the *Żandarmeria Wojskowa* (Military Gendarmerie – **ŻW**), a military police structure supporting discipline, security and order[40], and the *Wojska Specjalne* (Special Forces – **WS**), a branch of the Polish AF, composed of several elite units,

[37] As per the Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002 *(Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu)*.
[38] As per Art.º 6.º, item 2 of the Act of 24 May 2002.
[39] As per Art.º 9.º n.º 1 al. f) of *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 maja 2024 r. w sprawie ogłoszenia jednolitego tekstu ustawy o Straży Granicznej*.
[40] As per Act on the Military Gendarmerie and Other Law Enforcement Authorities of 24 August 2001 *(Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych).*

notably the *Grupa Reagowania Operacyjno-Manewrowego* (**GROM**), doing land and maritime counter-terrorism operations, and the *Jednostka Wojskowa FORMOZA* (**FORMOZA** Military Unit), a special operations unit of the Polish Navy, it is trained for maritime and underwater counterterrorism operations (EUROGENDFOR, 2025; *Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*; MND, 2025; MND, 2023; Zubrzycki, 2015).

Despite a low number of terrorist incidents, the significant proportion of arrests linked to extremist affiliations demonstrates Poland's proactive approach to threat anticipation and prevention (Olech, 2021). Its structured and coordinated response model may offer valuable lessons for countries like Portugal, particularly regarding the institutionalisation of multi-agency frameworks and the emphasis on early threat detection (Kochańczyk, 2020; Olech, 2021). For a systematised overview of Poland's counter-terrorism framework, including the key entities, their competencies and legal mandates, see Appendix D.2.

3.2.2. Legislative Framework

Poland's legislative response to terrorism is structured around a cohesive and strict legal framework, notably the Anti-Terrorism Act 2016 (*Ustawa o działaniach antyterrorystycznych*)[41], enacted in response to the growing external threat and the terrorist attacks experienced across the European Union (Olech, 2022b). This legislation grants the Forces and Security Services (SFS) extensive powers, including preventive detention for up to 30 days without immediate formal charges, restrictions on the stay of foreign nationals based solely on nationality and broad surveillance capacities such as interception of communications and access to personal data without prior judicial authorisation (Wiśniewski, 2018).

Complementing these measures is a special preventive detention regime in maximum-security institutions for individuals with irreversible psychiatric disorders and high-risk behaviour profiles, inspired by Norway's practices following the Breivik case (Wysocka, 2023; Zięba, 2015). These mechanisms aim to address modern terrorism's transnational, clandestine and digital nature, particularly Freelance Terrorism (Olech, 2022b).

Polish anti-terrorism legislation, especially the 2016 Act, has been internationally recognised for its robustness and design, receiving praise from institutions like the European Centre of Excellence for Countering Hybrid Threats, and is often cited as "the" model for other

[41] Amended in 2019 (*Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 4 kwietnia 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o działaniach antyterrorystycznych*).

EU member states (Wysocka, 2023). For further details on the operational mechanisms and legislative instruments, see Appendix D.2.

3.2.3. Absence of a Unified National Counter-Terrorism Plan

Poland currently lacks a unified national counter-terrorism plan, with the last strategic document being the "National Anti-Terrorist Programme for 2015-2019" (Resolution 252 of 9 December 2014) (Olech, 2022b; Wysocka, 2023). Although the programme aimed to diagnose threats and establish prevention guidelines, it was not renewed after its expiration. Despite this gap, Poland compensates through a robust legal framework, particularly the 2016 Anti-Terrorism Act, recognised as a model within the EU (Wysocka, 2023), and through highly specialised institutions like ABW and the TPCE (ABW, 2025; TPCE, 2021). These entities focus on prevention, public awareness and training.

Significant initiatives include the Terrorism Prevention Guide, a manual aimed at enhancing civilian preparedness and the "4U!" campaign, designed to educate the public on effective responses to terrorist incidents, including those involving firearms or hazardous substances (TPCE, 2021).

Despite the fact that Poland has a low level of terrorist threat, there is no immunity against it and a single radicalised individual is enough to cause a significant social impact. Even though Poland's response mechanisms are robust, the absence of an updated, centralised strategic plan may limit policy coherence and hinder a fully integrated national counter-terrorism strategy (Olech, 2022b). For further practical details on Poland's preventive initiatives and public awareness programmes, see Appendix D.2.

3.3. Mechanisms of France[42]

France is one of the European countries most exposed to and affected by recurrent terrorist attacks in the 21st century (Olech, 2022a), having suffered multiple high-profile and deadly incidents, such as the *Charlie Hebdo* attack (2015), the *Bataclan* massacre (2015), and the Nice truck attack (2016). The persistent nature of the terrorist threat has led the French State to adopt a robust counter-terrorism policy, grounded in enhanced legislative instruments, systematic surveillance and detention operations, and a highly centralised security coordination structure (Faustino, 2018). The objective is the eradication of the terrorist threat, reflecting the

[42] For detailed data on arrests, attacks, court cases and group affiliations in Portugal, Poland and France between 2013 and 2023, see Appendix E.

country’s continuous struggle against terrorism both domestically and internationally (Olech, 2021).

Throughout its history, it has experienced virtually every form of terrorism: anti-colonial terrorism in the 1950s; left-wing terrorism in the 1960s, notably in Corsica and the Basque Country; jihadist terrorism during the 1970s and 1980s; nationalist terrorism in the 1990s; and, in more recent times, religiously motivated terrorism (Olech, 2021, 2022a). Since 2015, it has witnessed a dual escalation of terrorist threats: domestic, and international. According to aggregated data from the TE-SAT reports by Europol (2014–2024), it recorded 415 terrorist attacks, the majority of which were separatist in nature (252), followed by right-wing inspired (76) and jihadist-inspired (74) incidents.

In terms of enforcement, 2.742 arrests for terrorist-related activities were recorded, 2.335 of which were linked to jihadist terrorism, and the remaining were associated with separatist (251), right-wing (118), left-wing (31), and other forms of terrorism (7). These arrests resulted in 1.002 court cases, of which 837 were jihadist-related, producing 948 convictions and 52 acquittals, equivalent to a very high conviction rate of 95%. This volume places France at the forefront of judicial and policing engagement with counter-terrorism in Europe. The high proportion of convictions relative to arrests suggests a consistent judicial response, while also highlighting the pervasiveness of radicalisation networks within the country.

Between 2014 and 2020, it recorded 116 terrorist incidents, confirming its position as one of the European countries most affected by this phenomenon. Of these incidents, 56% were attacks classified as armed assault, followed by 35% of bombings/explosions and 7% classified as facility/infrastructure attacks. These figures illustrate a high level of potential lethality, reflected in the 248 deaths and 1.009 injuries recorded during this period. The operational success rate of the attacks was 80%, revealing not only the frequency of the attacks, but also their effectiveness in achieving the attackers' immediate objectives. Most of the attacks were carried out by individual actors or small groups with a jihadist inspiration, often using automatic weapons, improvised explosives, or vehicles to run over people (tactics that correspond to the trends identified in Europol's TE-SAT reports). Comparison with other European countries shows that France faces a multidimensional and persistent threat, with diversified modus operandi and highly sophisticated logistical attacks. These factors explain the strong mobilisation of the French state in terms of surveillance, policing and legal mechanisms for prevention and repression.

3.3.1. Institutional Response

France's institutional counter-terrorism framework is characterised by an integrated and hierarchical network that ensures coordination across strategic, operational and tactical levels. Intelligence and external threat analysis are primarily the responsibility of the MND, through three key agencies: the *Direction Générale de la Sécurité Extérieure* (General Directorate for External Security – **DGSE**), which focuses on external intelligence gathering, counter-terrorism and cybersecurity (MND, 2025); the *Direction du Renseignement et de la Sécurité de la Défense* (Directorate for Defence Intelligence and Security – **DRSD**), responsible for defence counterintelligence (MND, 2025a); and the *Direction du Renseignement Militaire* (Directorate of Military Intelligence – **DRM**), which provides critical intelligence to support political and military decision-making (MND, 2025b). Internal security and the fight against terrorism fall under the remit of the MIA, with the *Direction Générale de la Sécurité Intérieure* (General Directorate for Internal Security – **DGSI**) as the main internal intelligence service, responsible for counter-terrorism, cybercrime and counter-espionage operations (MIA, 2025).

The *Ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique* (Ministry of Economy – **ME**) contributes through the *Direction Nationale du Renseignement et des Enquêtes Douanières* (National Directorate for Customs Intelligence and Investigations – **DNRED**), specialising in border security and the fight against organised crime and terrorism (ME, 2025a), and through the *Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins* (Intelligence Processing and Action Against Illicit Clandestins – **TRACFIN**), tasked with combating the financing of terrorism (ME, 2025b). At the judicial level, the MJ coordinates the criminal response through the *Parquet National Antiterroriste* (National Anti-Terrorism Prosecutor's Office – **PNAT**), responsible for prosecuting terrorism-related offences and the proliferation of weapons of mass destruction (MJ, 2019).

Operational counter-terrorism efforts are carried out mainly under the MIA. In contrast to Portugal, where the PJ operates independently, in France judicial police functions are integrated into the *Police Nationale* (French National Police – **PN**), through the *Direction Centrale de la Police Judiciaire* (Central Directorate of Judicial Police – **DCPJ**), and the *Gendarmerie Nationale* (French Gendarmerie – **GN**), through the *Sections de Recherches de la Gendarmerie Nationale* (Research Sections of the National Gendarmerie – **SRGN**). Key tactical units of PN include the *Brigades de Recherche et d'Intervention* (Research and Intervention Brigades – **BRI**), responsible for high-risk crisis situations; the **RAID** (*Recherche,*

Assistance, Intervention, Dissuasion – Research, Assistance, Intervention, Dissuasion), France's elite counter-terrorism and crisis response unit; and the *Compagnies Républicaines de Sécurité* (Republican Security Companies – **CRS**), a mobile corps specialised in public order and supporting anti-terrorism operations (PN, 2025a; PN, 2025b; PN, 2025c). The *Groupe d'Intervention de la Gendarmerie Nationale* (National Gendarmerie Intervention Group – **GIGN**) stands out for its advanced capabilities in land, air and maritime counter-terrorism operations, being recognised as the GN's elite unit and the preferred intervention force of the DGSE for missions abroad (MIA, 2025b; Olech, 2021).

Within the DGSI, the *Sous-Direction Anti-Terroriste* (Anti-Terrorist Sub-Directorate – **SDAT**) and the *Section Antiterroriste* (Anti-Terrorist Section – **SAT**)[43] both specialised in counter-terrorism efforts. They investigate both executed and planned terrorist attacks, with a preventive and pre-emptive focus. They are also responsible for conducting investigations linked to violence motivated by extremist ideologies (MIA, 2025c; MIA, 2024).

Inter-agency coordination was traditionally managed by the *Unité de Coordination de la Lutte Antiterroriste* (Coordination Unit for the Fight Against Terrorism – **UCLAT**), a central hub for threat assessment and information sharing, until its functions were transferred to the DGSI in 2019 (PoliceFR, 2025). The Ministry of Justice also plays a central role through the PNAT, ensuring consistency in judicial responses and issuing guidelines for terrorism prosecutions (*Loi n.° 86-1020 du 9 septembre 1986*).

France's counter-terrorism strategy is further distinguished by its strong emphasis on prevention, through reintegration centres, digital reporting platforms and community initiatives aimed at increasing resilience against radicalisation (Gouvernement Français, 2006; Faustino, 2018; Touati, 2023). France also advocates for robust digital surveillance powers to monitor extremist content online, although these measures raise concerns about fundamental rights (Gouvernement Français, 2006; Touati, 2023).

In sum, France's counter-terrorism framework is a paradigmatic example of an integrated, hierarchical and multidimensional model, enabling a swift, coordinated response to terrorist threats while provoking ongoing debates regarding its implications for individual freedoms. For a systematised overview of France's counter-terrorism framework, including the key entities, their competencies and legal mandates, see Appendix D.3.

[43] SAT functions as the Paris Police counterpart to the SDAT.

3.3.2. Legislative Framework

France's legislative framework for counter-terrorism has evolved significantly, particularly after the jihadist attacks of 2015. A decisive milestone was the enactment of Law n.º 2017-1510, known as the *loi SILT*[44], which incorporated into ordinary law several emergency powers initially used during the state of emergency. These include warrantless home searches, administrative house arrests, closure of places of worship promoting extremism and expanded surveillance capabilities based on algorithmic analysis (Faustino, 2018; Olech, 2022a).

Additional legislative developments focused on reinforcing border controls and introducing post-release administrative measures targeting individuals convicted of terrorism-related offences (Olech, 2022a). The French Penal Code, under Titles II ("*Du* Terrorisme") and III ("*Des atteintes à l'autorité de l'État*"), consolidates severe penalties for the commission, incitement, financing and indirect support of terrorist activities (Code Pénal, 2022)[45]. Strategic planning is supported by the *Livre Blanc sur la sécurité intérieure face au terrorisme*, which outlines doctrines for threat anticipation, prevention, and coordinated responses (Gouvernement Français, 2006). Complementing the legal framework is the FSPRT (*Fichier de Traitement des Signalements pour la Prévention de la Radicalisation à Caractère Terroriste*), a database coordinated by the DGSI to monitor and address radicalisation risks through multi-agency interventions (Gouvernement Français, 2006). The FSPRT supports a preventive, multi-agency approach, enabling tailored monitoring and psycho-social interventions through local evaluation groups chaired by prefects, by focusing on radicalisation risk rather than police investigation.

France's model is characterised by a robust and far-reaching legal architecture, praised for its effectiveness but also subject to criticism from human rights organisations concerning the balance between security and civil liberties (Gouvernement Français, 2006). For a detailed breakdown of the French counter-terrorism legislative instruments and preventive mechanisms, see Appendix D.3.

[44] See *Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*.
[45] As per Art.º 113-13 (penal law also applies to terroristic acts); Art.º 227-24 (the incitation to terrorism to minors is penalized with a prison sentence of 3 years and 75.000 euros fine); Art.º 421-1 to 422-7 (the terroristic acts); Art.º 434-2 and Art.º 434-6.

3.3.3. Plan Vigipirate and Operation Sentinelle

France's counter-terrorism strategy relies heavily on two operational frameworks: the *Plan Vigipirate* and *Operation Sentinelle*. The *Plan Vigipirate* functions as a dynamic national alert system, structured around three escalating levels of security measures[46] aimed at protecting critical infrastructure, public spaces and ensuring the continuity of state functions (SGDSN, 2016). It integrates the participation of state institutions, private actors and civil society, promoting public vigilance through awareness campaigns such as the "assume, alert, protect" initiative (SGDSN, 2016; Olech, 2022a). This permanent framework adapts to the threat level and encompasses more than 300 specific measures across different sectors.

Complementing it, *Operation Sentinelle*, launched in 2015 after the *Charlie Hebdo* attacks, mobilises between 7.000 and 10.000 military personnel throughout the national territory. These forces, operating under strict legal limitations, patrol high-risk sites and provide immediate response capabilities in coordination with the PN and the GN (Troin & Léonard, 2016; SGDSN, 2016; Olech, 2022a). Soldiers have limited law enforcement powers, being authorised only to use lethal force in imminent threat situations. Together, *Plan Vigipirate* and *Operation Sentinelle* exemplify France's integrated model of civil-military cooperation in counter-terrorism, balancing preparedness and deterrence while raising debates about the preservation of civil liberties. For a detailed overview of these frameworks and their operational dynamics, see Appendix D.3.

3.4. Comparison and Cooperation

3.4.1. Comparative Analysis of Institutional Responses

The institutional frameworks of Portugal, Poland and France reveal distinct national models of counter-terrorism governance, shaped by their historical trajectories, security cultures and constitutional structures. France adopts a bifurcated intelligence architecture, distinguishing between internal and external threats via the MIA (DGSI) and MND (DGSE, DRM and DRSD), respectively. This contrasts with Poland's centralized model, where both ABW and AW fall under the authority of the PM. Portugal also concentrates strategic oversight in the PM office via SIRP, which supervises SIS and SIED. At the prosecutorial level, France stands out with the PNAT, a highly specialised and exclusive body for terrorism-related

[46] The levels of alert are: "Vigilance"; "Enhanced Security – Risk of Attack"; "Emergency Attack" (SGDSN, 2016)

offences. Portugal, through the DCIAP, ensures central coordination but without a dedicated anti-terrorism branch. Poland relies on regional prosecutors working closely with ABW, a model that may risk fragmentation in complex cases.

Tactically, all three states deploy elite counter-terrorism units, however, France and Polan concentrate tactical response within unified entities, whereas Portugal divides responsibility between the PSP and GNR. As for intelligence-police integration, Poland and France assign judicial competences to their intelligence services (ABW and DGSI), while Portugal maintains a strict separation, with SIS focused on prevention and PJ conducting criminal investigations.

These institutional divergences are not merely administrative, they reflect national interpretations of the balance between security and civil liberties, the roles of intelligence versus police authorities, and the place of military structures in the domestic counter-terrorism arena. A systematised comparative overview of the institutional models of the three countries is presented in Appendix D.4.

3.4.2. Comparative Analysis of Legislative Frameworks

The legislative frameworks of Portugal, Poland and France reveal divergent approaches to counter-terrorism, reflecting distinct legal cultures, security doctrines and historical experiences. Portugal maintains a highly legalistic and tights-oriented model, with robust judicial oversight and traditional criminal law instruments, yet with limited scope for preventive action outside formal inquiries. Poland, in contrast, adopts a securitarian framework, granting sweeping administrative powers to security forces under the 2016 Anti-Terrorism Act, including extended surveillance, prevention detention and data collection without judicial warrant. France's legislative approach has progressively absorbed exceptional measures into ordinary law through the *loi SILT* and related instruments, establishing a hybrid model that prioritises rapid intervention and public safety, albeit with partial judicial control and recurring criticism from civil rights groups. A systematised comparative overview of the legislative frameworks of the three countries is presented in Appendix D.4.

3.4.3. International and European Cooperation

International and European cooperation constitute a key pillar of counter-terrorism strategies in Portugal, Poland and France. These countries participate in various multilateral frameworks aimed at enhancing intelligence sharing, joint operations and strategic

coordination. At the European level, initiatives led by Europol and the ATLAS Network foster collaboration among member states, particularly in information exchange and tactical training. Global cooperation is strengthened through Interpol and the United Nations Counter-Terrorism Centre (UNCCT), promoting common standards and preventive strategies.

Furthermore, alignment with the European Union's Security Union Strategy 2020–2025 ensures a coordinated response to emerging threats, including cyberterrorism and hybrid attacks (European Commission, 2020). These mechanisms not only enable rapid operational responses but also facilitate the transfer of knowledge and best practices, reinforcing the multilateral dimension of national counter-terrorism efforts. For an overview of the main international cooperation platforms and mechanisms, see Appendix D.4.

PART II – METHODOLOGICAL FRAMEWORK AND DISCUSSION OF RESULTS

CHAPTER 4 – METHODOLOGY, METHODS AND MATERIALS

Following the completion of Part I, which established the theoretical framework, this chapter presents and justifies the methodological choices underlying this study. In line with Santos & Lima (2019, p. 25) and Saunders *et al*. (2009), the selected methodology constitutes the strategic plan designed to coherently address the research objectives and questions. The approach adopted integrates the theoretical and empirical dimensions, ensuring that the methods, techniques and data collection procedures are aligned with the research problem and objectives (Patton, 2015), thereby safeguarding the scientific rigour and validity of the study.

4.1. Research Questions, Research Objectives and Analytical Model

Following the definition of the research topic and object, it is essential to establish the central problem that guides the analysis. In line with Sarmento (2013) and Quivy & Campenhoudt (2008), the formulation of a clear Central Research Question (CRQ)[47] enables the structuring of coherent objectives and research questions. Accordingly, this study formulates the following CRQ: "**How can Freelance Terrorism be best prevented and countered in Portugal, based on the case studies of Poland and France?**".

The CRQ is operationalised through a General Objective (GO), which is further broken down into Specific Objectives (SO) that give origin to the Derived Questions (DQ) (Gil, 2008). This structuring allows a methodical and coherent development of the research process, as advocated by Baptista & Sousa (2011) and Gil (2008), ensuring alignment between the research questions, objectives, and methodological strategies.

Fortin (1999) argues that the achievement of the objectives is directly proportional to the extent to which the research questions are addressed, as the objectives may be considered fulfilled once the respective questions are adequately answered. In this sense, the analytical model developed and all the methodological framework for the present study is presented in Appendix H.

[47] CRQ guides the entire logical and analytical structure of the study and to which a comprehensive answer is sought (Prodanov & Freitas, 2013).

4.2. Methodological Approach

The methodological approach adopted in this research is intrinsically linked to the nature of the research object and the instruments selected for data collection (Rosado, 2017). An inductive reasoning method was employed, allowing theoretical generalisations to be drawn from specific observations and data (Santos & Lima, 2019). This approach was operationalised through the analysis of legislative mechanisms and institutional strategies in Portugal, Poland and France, combining documentary analysis and semi-structured interviews.

Given the complexity of the phenomenon, a qualitative approach was prioritised, aiming for an in-depth understanding of institutional practices and participants' perspectives, rather than statistical generalisation (Vilelas, 2020). However, quantitative and statistical interpretation supported critical reflection on the results (Patton, 2015). Semi-structured interviews complemented the documentary analysis, enhancing the triangulation of data sources and collection methods. In terms of the research problem, an inductive reasoning approach was followed, which enables the construction of theoretical generalisations starting from the observation and analysis of specific data and results (Rosado, 2017, p. 118; Santos & Lima, 2019)

A cross-sectional research design was adopted, allowing data collection at a specific point in time and enabling the identification of patterns across the analysed cases (Santos & Lima, 2019). The focus was the analysis of strategies for preventing and combating Freelance Terrorism in Portugal, based on a comparative study with Poland and France. Details regarding methodological triangulation and interview logistics are provided in Appendix F.1 and Appendices H and I.

4.3. Data Collection Method

To deepen the knowledge base and ensure methodological rigour, data collection was grounded in the nature of the research problem, combining documentary analysis, observation and gathering of information via semi-structured interviews – qualitative strategy (Fortin, 1999; Santos & Lima, 2019). Documentary analysis enabled the collection and systematisation of data from reports, regulations, academic publications, and official documents, with priority given to primary sources[48], using secondary materials only when the first were insufficient (Sarmento,

[48] Freixo (2011) explains that primary sources are documents that have not been interpreted by other authors, whereas secondary sources consist of data "that has already been collected and analysed by someone else"

2013, p. 27; Kothari, 2004, p. 111). This analysis enabled partial answers to be provided for the previously defined DQ. In addition, international practices and strategies for the prevention of Freelance Terrorism were identified and examined.

Semi-structured interviews were conducted using pre-established open-ended questions tailored to two distinct respondent groups, facilitating in-depth exploration and the collection of complementary data (Santos & Lima, 2019; Prodanov & Freitas, 2013). Interviewees were contacted via institutional channels, ensuring informed consent and guaranteeing confidentiality. For detailed information regarding the primary databases, the selection and grouping of documentary sources, as well as the operational procedures followed during the interview process, see Appendix F.2. Additionally, the structure of the analytical model and the categorisation of documentary sources are available in Appendix H.

4.4. Sampling

The sampling process adopted in this study followed a non-probability strategy, specifically combining convenience and purposive sampling. Participants were intentionally selected based on their professional experience and institutional relevance to the phenomenon of terrorism, prioritising depth and relevance over statistical representativeness (Fortin, 1999; Gil, 2008; Santos & Lima, 2019; Rosado, 2017) The universe consisted of institutions and professionals from Portugal, Poland and France, with a sample comprising representatives from operational and strategic bodies. While interviews were successfully conducted in Portugal and Poland, French authorities formally declined participation, a limitation that is acknowledged in the study (see Appendix H for mor detail).

For this research, three distinct Interview Guides (IG Types A, B, and C)[49] were developed, each adapted to the national context of the respondents. Each interview was preceded by a Letter of Introduction, and anonymity and informed consent were strictly ensured. A detailed description of the interview procedures, including the structure of the Interview Guides (IG) and the anonymisation process, can be consulted in Appendix I.

The complete list of entities contacted and the characterisation of the interviewees are presented in Appendix H and J. Additionally, for a detailed explanation of the theoretical definitions and concepts underlying the sampling strategy, refer to Appendix F.3.

(Kothari, 2004, p. 111). Therefore, primary sources were prioritised using secondary sources only when the first failed to provide sufficiently relevant or up-to-date information (Sarmento, 2013).

[49] *Vide* Appendix I for full Interview Guides and Appendix F.3.

4.5. Data processing and analysis techniques

The interview data were processed and analysed through a qualitative Content Analysis (CA) approach, appropriate for interpreting respondents' experiences and identifying thematic patterns (Charmaz, 2004; Sparkes & Smith, 2014 cited in Resende, 2016). Although primarily qualitative, quantitative elements, such as the frequency of terms, were incorporated to reinforce consistency (Resende, 2016). The ITCI method (Interview, Transcription, Categorisation, and Interpretation) structured the analysis process (Resende, 2016), transforming interview transcripts into analytical categories aligned with methodological principles of homogeneity, exclusivity, objectivity and exhaustiveness (Johnson & Christensen; 2014). Thus, the IGs were developed and validated, representing the first stage of the ITCI process. The MAXQDA software was used to facilitate efficient coding, cross-referencing and data management[50].

Following Guerra's (2006) framework[51], the analysis progressed through full transcription, exploratory reading, descriptive and interpretive analysis. Responses were grouped into categories and subcategories according to the DQ and SO, ensuring theoretical alignment and methodological rigor. For a detailed description of the ITCI method, coding process, and operational procedures, see Appendix F.4. The coding matrices, summary tables, and full categorisation schemes are available in Appendix J.

[50] Johnson & Christensen (2014) emphasise that coding must enable the classification of relevant data into mutually exclusive and theoretically meaningful categories.
[51] See Appendix F.4.

CHAPTER 5 – PRESENTATION, ANALYSIS AND DISCUSSION OF RESULTS

This chapter presents the results obtained through fieldwork, consisting of two semi-structured interview surveys with counterterrorism experts. IGs were linguistically and contextually adapted to the Portuguese, French and Polish frameworks but included a core set of questions to ensure consistency and enable comparative analysis (see Appendix G for a detailed description of the IG development, data analysis methodology, and lexical similarity results). The interviews aimed to explore institutional perspectives on the definition, prevention and combat of Freelance Terrorism, as well as the operational, legal, and interinstitutional frameworks in each national context. The questions were designed to address the DQs and the CRQ, with a detailed correspondence available in Appendix H.

Content analysis was performed using MAXQDA software, based on pre-defined categories and subcategories. Each response was segmented into contextual and register units to facilitate thematic interpretation and quantitative comparison. Additionally, lexical similarity between interviewees was calculated, revealing low coefficients (between 0,036 and 0,175) and indicating significant variation in vocabulary, thereby reflecting the complex and non-normative nature of Freelance Terrorism. Pearson correlation coefficients based on the repetition of words and expressions further supported this observation.

A characterisation of interviewees and a detailed list of coded units and excerpts is provided in Appendix J, along with the quantitative analysis of segment frequencies. The interview guides are included in Appendix I. The following sections present and analyse the responses by interview question, supported by tables and visualisations to highlight key patterns.

5.1. Analysis and Discussion of Interview Guide Type A (Portugal)

This subchapter presents the analysis and discussion of the results obtained from IG Type A, conducted with three key national actors involved in counter terrorism in Portugal: E1, E2 and E3. The objective was to understand their institutional perspectives regarding the definition, prevention and combat of Freelance Terrorism, as well as their operational, legal and interinstitutional frameworks.

All interviewees articulated complementary institutional roles to **Question 1**. E1 emphasised UCAT's coordination mandate and information exchange mechanisms (33% of coded segments) while E2 underscored strategic intelligence production. E3 focused on first-line operational response. This thematic fragmentation reflects the sectorial specialization of each entity, although a more integrated articulation of role could be desirable.

In **Question 2**, although the terminology varies, E2 and E3 converged on a general definition of Freelance Terrorism as ideologically inspired individual or small cell action (67%), while E1 maintained a broader and less typologised perspective. The lack of a unified conceptual approach can make it difficult to harmonise inter-institutional responses.

While E1 refrained from extrapolating profiles (33%), E2 and E3 shared the concern about the online radicalisation of young people (67%) in **Question 3**. However, the absence of concrete national cases weakens empirical validation and suggests a dependence on European trends to mould local threat perceptions.

The answers to **Question 4** were divergent: E1 explicitly refused to draw conclusions due to insufficient data, while E2 and E3 pointed to digital radicalisation and EU standards as indicative of an increased risk. This highlights a gap between operational prudence and strategic projection.

The interviewees highlighted different strategies when answering **Question 5**: E1 referred to ENCT 2023 as a guiding framework, E2 to intelligence monitoring and E3 to training, the use of OSINT and awareness-raising campaigns. It should be noted that E3 was responsible for the majority of references coded in this section (67%), which reflects greater operational involvement. However, this disparity may indicate uneven institutional investment in prevention.

Although all the interviewees recognised the importance of rapid tactical responses in **Question 6**, only E2 and E3 described concrete mechanisms, such as intelligence-led operations and confidential coordination plans. E1 relied on broader references to strategic documentation. This may suggest different degrees institutional mandates.

To the **Question 7**, all confirmed structured coordination (100%). E1 detailed the UCAT technical team and the meeting schedule; E2 referred to comprehensive coordination frameworks; E3 pointed to restricted operational plans. The solidity of this co-operation was evident, although its confidential nature limits transparency and public scrutiny.

There was total consensus (100%) on the international exchange of information mentioned in **Question 8**, mainly through Europol. However, only E2 specified platforms such

as the Counter Terrorism Group and Berna Club, and E3 emphasised the strategic importance of TE-SAT Reports. This suggests the need for a more standardised framework for international involvement.

Once again, all the interviewees rated international co-operation positively (100%) in **Question 9**. However, none were able to articulate concrete protocols with France or the GNR. This raises concerns about the depth and specificity of bilateral co-operation beyond declarative alignment, even though it's known that they exist.

In **Question 10**, while E2 and E3 identified legal and procedural obstacles (67%), E1 made no comment. The gap between legal harmonisation and practical coordination remains a structural challenge in the EU's security architecture.

To **Question 11**, in general, interviewees assessed the legislation as adequate (67%), but identified areas for improvement. E1 advocated revising the 2016 decree governing UCAT, while E3 suggested reforms in line with digital threats. The lack of legal adaptation to rapidly evolving phenomena, such as online radicalisation, was a shared concern.

There was unanimity on the critical challenge of early detection (100%) posed with **Question 12**. Other difficulties include online anonymity, encryption and low public awareness. The absence of recorded incidents creates risks of complacency and hinders the urgency of defining policies.

All the interviewees in **Question 13** stressed the importance of frontline staff (100%), particularly in recognising signs of radicalisation. E3 emphasised the importance of all agents, even off-duty ones, as potential informers. This ordinary perspective reinforces the importance of bottom-up contributions to national security.

In **Question 14** only E2 and E3 mentioned HUMINT and OSINT (67%), recognising their usefulness and limitations. The challenge is to collect meaningful data while respecting legal limits and avoiding prejudice.

All interviewees recognised the potential of AI, posed in **Question 15**, in data analysis and online monitoring (100%), although applications remain in exploratory stages. Ethical, legal and operational concerns were the most common reservations.

To **Question 16**, E1 refrained from commenting, while E2 and E3 described it as an effective and adaptable model (67%). E3 also emphasised the deterrent effect of the plan after the 2015 attacks. The potential for inspiration exists, but requires contextual adaptation.

E2 and E3 supported the idea mentioned in **Question 17**, citing the benefits of preparedness and public involvement (67%), but stressed the need to adapt any strategy to national threat levels and the social context.

Proposals asked in **Question 18**, include revising outdated legislation, investing in training and digital literacy and strengthening society's resilience (67%). E3 cited raising the alert level to 3 – Significative, after the Hamas attacks in 2023 as a turning point.

In the **Question 19**, E1 and E2 mentioned the value of academic involvement and the participation of civil society (67%). The tension between institutional discretion and public discourse was implicitly recognised.

In short, this analysis highlights the diverse but complementary perspectives of Portuguese actors in the fight against terrorism. Despite low lexical convergence (Appendix J), thematic overlaps, especially in prevention, legal adequacy and international co-operation, its revealed emerging patterns of consensus. However, asymmetries in the depth and specificity of responses suggest the need for greater harmonisation and transparency in national and international efforts to combat terrorism. For a more in-depth analysis of the analysis of IG Type A, see Appendix G.1.

5.2. Analysis and Discussion of Interview Guide Type C (Poland)

This subchapter analyses the responses from IG Type C, applied to two operational agents from elite Polish units: E4 and E5. Their testimonies offer critical insights into the perception and strategic posture of Polish security forces regarding Freelance Terrorism, illustrating both institutional strengths and emerging vulnerabilities.

In **Question 1**, Both respondents emphasise their unit’s relevance within Poland’s counter-terrorism structure. E4 (50%) describes a direct tactical response role, while E5 (50%) adopts a more strategic posture encompassing prevention and special operations. Codings 1.1 and 1.2 confirm functional complementarity but suggest a division of responsibilities: E4 executes, E5 anticipates. This divergence underscores the layered architecture of Poland’s counter-terrorism model: reactive at the tactical level and anticipatory at the strategic.).

Both interviewees aligned themselves in defining freelance terrorism, in **Question 2**, as perpetrated by self-radicalised individuals or small, unaffiliated groups, often through digital environments. However, E5's articulation is broader, noting the absence of structured support as a key detection challenge. Their alignment reveals a shared institutional awareness of digital radicalisation as a central feature.

In **Question 3**, 60% of the coded units (3.1 to 3.5) were mentioned, indicating moderately shared insights. Both identify online radicalisation as a primary vector. E4 focuses on digital surveillance of isolated individuals, while E5 highlights disguised infiltration via refugee routes. E5 also raises concerns about border destabilisation and ideological camouflage, illustrating a broader security framing. The thematic distinction reflects their differing institutional remits but also a common perception of emerging risk vectors.

In **Question 4** both interviewees describe a context of growing concern, linked to global radicalisation dynamics and increased access to extremist content. E5 highlighted the accessibility of low-tech tools and online indoctrination.

In **Question 5**, E4 referred to indirect support through preparedness, while E5 outlined specific preventive measures such as sensitisation, intelligence-led policing and early intervention. The coding shows E5's broader institutional investment in upstream prevention.

Both emphasised tactical response to confirmed threats in **Question 6**, although E5 added HUMINT and scenario-based simulations. While the quantitative balance is somewhat equal, E5's responses show greater operational depth, even though it's shown complementarity rather than redundancy in combat strategies.

Both interviewees, in **Question 7**, described a robust, centralised coordination mechanism through intervention forces and control centres, which represent 100% agreement between the units. Joint training, planning and shared communication systems are emphasised, suggesting maturity in national interinstitutional cooperation.

Both emphasised the importance of intelligence exchange, particularly through Europol and Frontex, in **Question 8**. E5 frames Poland's geography as increasing its relevance in cross-border threat detection. The coding indicates a high degree of alignment and institutional integration in European intelligence frameworks.

To **Question 9**, both interviewees referred to general EU co-operation as constructive, but noted limited involvement with Portugal. E5 mentioned the potential for bilateral improvement. Their answers suggest an untapped space for operational synergies.

Both E4 and E5 mentioned linguistic, legal and procedural discrepancies and communication problems, when answering **Question 10**. These common concerns represent 100% of the units coded and reflect common structural obstacles at EU level. E5's inclusion of digital priorities and structured coordination with Portugal (10.2) suggests a nuanced grasp of transnational complexity.

Again, in **Question 11**, existed a 50% convergence (11.1 shared; 11.2 only in E5). Both considered the Polish framework to be adequate, but in need of continuous adaptation. E4 perceives existing frameworks as adequate, while E5 calls for more agile procedures and digital adaptability emphasising the need to safeguard civil liberties in the context of technological expansion. This contrast points to a strategic versus tactical lens on legislative adequacy.

Regarding **Question 12**, E4 and E5 identified early detection, anonymity and low public awareness as the main challenges. E5 adds encrypted communications and the dark web, which suggests greater maturity in threat modelling.

For **Question 13**, the consensus was total (100%) on unit 13.1. Both consider frontline personnel to be critical sensors. E5's additional reference to community trust emphasises relational intelligence.

E4 and E5 totally agree (100%) on the strategic value of HUMINT, in **Question 14** OSINT, SIGINT and behavioural analysis are mentioned by E5, revealing a more in-depth analysis on the question. Legal restrictions were frequently cited by both, pointing to an ethical-operational tension in the use of intelligence services.

To **Question 15**, coded units 15.1 and 15.2 were mentioned by both, considering AI to be promising, especially for predictive analysis. However, the current application in Poland is still exploratory. E5 explicitly mentions bias and human supervision as critical challenges.

Only E5 addressed unit 16.3 in **Question 16**, mentioning the risks of excess, revealing a deeper reflection on proportionality. While both recognise the deterrent value of the *Vigipirate* model, E5 stresses the need for socio-political adaptation before implementation to combat Freelance Terrorism.

In **Question 17**, E4 and E5 identified the value of adapting such models (17.1 and 17.2). Only E5 mentioned the need for culturally sensitive implementation (17.3), reaffirming its broader conceptual understanding of international policy transfer.

To **Question 18**, the two shared units (18.1 and 18.2) reflecting a convergence on early detection and coordination between agencies. However, unit 18.3 was only mentioned by E5, pointing to their broader vision regarding public resilience, investment in deradicalisation programs and international alignment.

In **Question's 19**, units 19.1 to 19.6 show that both interviewees had very asymmetric, yet valuable and complementary views. Themes included disinformation, hybrid threats and building trust at the local level. E4 centred on officer's well-being (mental health), public education and enhancement on international cooperation in digital surveillance. E5 opted to

address the hybrid threats and foreign disinformation, that prevention should be prioritised over reaction and that the trust between police and local communities should be strengthened.

Thematic analysis of IG Type C reveals partial convergence between E4 and E5 in most categories, especially with regard to institutional coordination, international frameworks and operational challenges. However, differences emerge in the strategic breadth and depth of commitment. E5 consistently articulates a more systemic and preventive stance, while E4 maintains a reactive and execution-centred approach. The low lexical similarity (Appendix J) supports the finding of institutional divergence. This variation, rather than being problematic, reinforces the notion that national counterterrorism ecosystems benefit from functional diversity. For a more in-depth analysis of the analysis of IG Type C, see Appendix G.2.

5.3. Comparative Analysis: Portugal vs Poland

The comparative analysis between IG Type A and Type B reveals both convergences and divergences in institutional perspectives regarding Freelance Terrorism. While some shared thematic axes are apparent, particularly regarding definitions, coordination and detection, clear distinctions emerge in terms of institutional posture, conceptual maturity and operational emphasis. The entities interviewed in Portugal presented a more segmented model with differentiated roles, from strategic coordination and intelligence to operational deployment, with evident fragmentation. In contrast, the Polish entities illustrated layered but more integrated model, where operational units are simultaneously involved in preparedness, response and strategic foresight. This difference may reflect Portugal's reliance on inter-agency coordination versus Poland's consolidation of strategic and tactical functions within elite units.

Conceptually, both countries converge on the definition of Freelance Terrorism as a digitally mediated, ideologically driven phenomenon involving individuals or small groups. However, Polish respondents provided more operationalised profiles and detection challenges, particularly regarding border infiltration and the refugee crisis, something not mentioned in the Portuguese data. In this turn, Portugal's conceptualisation appeared more abstract, possibly due to the lack of recent national attacks.

Preventive strategies show marked divergences. Portuguese actors referenced ENCT, institutional training, and OSINT monitoring. Polish actors offered a broader array of upstream measures, including public engagement and behavioural detection, particularly E5. The thematic coding suggests that Polish prevention is more embedded in operational culture, whereas Portuguese efforts remain somewhat policy-oriented. In terms of combat mechanisms,

it's possible to affirm that both counties emphasised intelligence-led intervention, with Polish actors giving more use to simulation and HUMINT, while Portuguese actors remained more generic or policy-referential.

Institutional coordination and international cooperation had strong convergences, in the sense that both countries reported structured national coordination and active participation in platforms like Europol and Frontex. In legal terms, both countries considered their frameworks broadly adequate but in need of evolution, meaning that it was stressed the urgency of adapting to digital threats and balancing security with civil liberties, especially nowadays. Operational challenges were consistently highlighted across contexts, with early detection and online anonymity, even though Polish actors offered a more insightful perspective in to the digital and decentralised radicalisation channels of the phenomenon.

When discussed the role of individual agents, both contexts affirmed the importance of frontline vigilance. Yet, Polish discourse was more community-oriented, suggesting a shift toward relational intelligence and local trust. Both recognised the value of HUMINT, AI and digital tools, although implementation remains limited. Polish responses appeared more technologically grounded and ethically reflective, citing concerns around algorithmic bias and data protection. Finally, while both sets of respondents saw merit in adopting elements of France's *Plan Vigipirate*, they also offered a more critical and contextualised view of its applicability, mentioning the importance of adapting it to each national reality.

In summary, while Portugal and Poland share key strategic concerns, their institutional responses to Freelance Terrorism are shaped by distinct operational logics. Portugal's model is anchored in coordination and normative frameworks, while Poland's favours operation integration and anticipatory posture. This diversity, as shown by lexical divergence in Appendix J, should not be seen as a weakness but as an indication of functional complementarity across the EU counter terrorism ecosystem. For a more in-depth comparative analysis, see Appendix G.3.

5.4. Answers to Derived Questions

This subchapter aims to provide a critical and integrated response to the DQ's, based on the triangulation of the empirical material from IG Type A and C, the correlation matrices (Appendix J) and the theoretical framework developed in Part I.

DQ1: How can Freelance Terrorism be best investigated in Portugal? The effective investigation of Freelance Terrorism in Portugal requires a multidimensional and adaptive

approach, as suggested by both theoretical insights and the empirical evidence gathered through IG Type A. The decentralised, ideologically fluid and digitally embedded nature of this type of terrorism, as outlined by Silva (2020) and (Cortez, 2021; Lopes, 2019; OSCE, 2014; Silva, 2020), presents serious challenges to conventional investigative strategies that rely on structured affiliations and pre-existing intelligence networks.

The Portuguese interviewees (E1-E3) presented varied yet complementary perspectives. E1 underscored the centrality of UCAT's coordination mandate and information exchange mechanisms, yet did not provide detail on specific investigative procedures (code 1.1). E2 and E3, however, stressed the importance of intelligence-led policing, OSINT-based monitoring of online environments and the integration of behavioural indicators into surveillance strategies (codes 14.1, 14.3). This indicates that the investigative focus is currently more attuned to digital observation and inter-institutional coordination that to proactive infiltration or pre-emptive neutralization.

From a strategic standpoint, the ENCT offers a foundation for multi-agency investigation. However, gaps persist. E3 highlighted the need for better training of first-line operatives in identifying early signs of radicalisation (code 13.1), while E3 emphasised the limited capacity to act in pre-criminal phases due to legal and ethical constraints (code 11.2, 11.3, 11.4). These limitations reflect he broader European tension between investigatory reach and rights protection, as discussed by OSCE (2014), Lopes (2019), Silva (2020) and Cortez (2021).

The Portuguese legal framework, although generally considered adequate by respondents (code 11.1), appears outdated in critical areas such as encrypted communications, AI-based surveillance and online propaganda countermeasures. Also, as mentioned by Silva (2015), the legal regime governing vehicle searched, the regime of communications interception and the imprisonment penalties for terrorism acts should be revised.

The investigation of Freelance Terrorism in Portugal would, therefore, benefit from: i) expanding OSINT and behavioural analytics units, particularly within the UCAT and operational branches like the GNR; ii) promoting targeted and continuous training for agents at all hierarchical levels, focusing on early-stage detection and online behavioural indicators (code 13.1); iii) Enhancing legal mechanisms to enable lawful action during the radicalisation process particularly in encrypted digital contexts; iv) Deepening cooperation with EU intelligence structures (i. e. Europol), while institutionalizing bilateral protocols that go beyond declarative

alignment; v) Investing in predictive risk modelling through AI, combined with robust ethical oversight and TRAP-18 (Meloy, 2021) and HCR-20 v3 (Douglas *et al*., 2014).

DQ2: How can Freelance Terrorism be best investigated in Poland? Investigating Freelance Terrorism in Poland requires a multi-layered strategy that integrates early behavioural detection, inter-agency intelligence coordination, and legal-technical adaptability. The empirical data from IG Type C, triangulated with the theoretical literature (Part I), reveal a robust, albeit evolving, national approach.

Firstly, early detection remains paramount. Polish respondents E4 and E5 repeatedly stressed the difficulty of identifying isolated individuals lacking organisational affiliation, particularly in online environments where radicalisation occurs through gaming platforms, encrypted chats and disinformation channels (codes 3.1, 3.2, 3.4, 12.1, 12.2). E5, in particular, highlighted the value of community-level monitoring, psychological vulnerability indicators and behavioural anomalies, aligning with Cortez (2021), Silva (2020), Olech (2022a), Zubrzycki (2017), Wiśniewski (2018) and TPCE (2021), who stress the shift from hierarchical organisational mapping to individualised radicalisation trajectories. The operational use of HUMINT, OSINT and scenario-based simulations (codes 6.2, 14.1, 14.2) suggests a preventive orientation rooted in anticipatory intelligence.

Secondly, the Polish model benefits from highly integrated intelligence frameworks. Interviewees reported centralised coordination between tactical units, national command centres, and EU-level structures such as Europol and Frontex (codes 7.1, 8.1). This interinstitutional maturity is further enhanced by the work of the TPCE, operating under the ABW, which serves as a national and international benchmark for research, training and operational guidance in counter-terrorism. The TPCE's role in integrating behavioural science, digital forensics and simulation-based profiling strengthens Poland's capacity to detect decentralised threats in real time (TPCE, 2025; TPCE, 2021). This model reflects a European paradigm of multi-scalar governance (Zubrzycki, 2015; Puacz-Olszewska, 2019), where in national infrastructures merge with supranational security protocols.

Thirdly, legal adaptability is crucial. Although the Polish legislative framework is broadly considered adequate (code 11.1), E5 advocated for reforms addressing encrypted communication, algorithmic surveillance and artificial intelligence ethics. These concerns echo theoretical tensions regarding the balance between proactive investigation and civil liberties (Olech, 2022b) . Nonetheless, as Wysocka (2023) observes, Polish counter-terrorism legislation remains among the most comprehensive in Europe, enabling not only reactive but also

preventive and pre-emptive action with judicial oversight. The sophistication of legal instruments, including those allowing coordination between police and intelligence agencies, provides a strong normative backbone for investigative operations.

In summary, the investigation of Freelance Terrorism in Poland relies on a hybridised model combining community-based early warning, centralised intelligence orchestration and technologically informed legal structures. The inclusion of institutions like the TPCE, combined with one of the most advanced legal frameworks in Europe (Wysocka, 2023), positions Poland at the forefront of proactive counter-terrorism investigation. While challenges remain, particularly in digital detection and ethical oversight, Poland's layered and anticipatory approach sets a European benchmark for confronting decentralised, ideologically driven threats.

DQ3: How can Freelance Terrorism be best investigated in France? Investigating Freelance Terrorism in France requires a multidimensional strategy rooted in institutional experience, legal sophistication and technological integration. Given France's status as one of the EU's most targeted countries by decentralised terrorist threats (CEU, 2005; EUROPOL, 2014-2024), the state's counter-terrorism architecture reflects a high level of preparedness, centralisation and anticipatory logic.

As outlined in Part I, France benefits from a multi-agency approach involving entities such as the DGSI, the PNAT and the Anti-Terrorist units from GN and PN with the judiciary functions. These entities operate under an integrated intelligence and criminal justice system, which enables efficient communication and procedural acceleration when addressing individuals suspected of radicalisation. The FSPRT, a national registry dedicated to individuals flagged for extremist tendencies, plays a pivotal role in facilitating pre-emptive investigations even in the absence of direct criminal links (DGSI, 2024).

This institutional design corresponds to Olech (2022a) anticipatory model of intelligence, which advocate for strategic foresight, layered coordination and the active use of behavioural signals in identifying threats. Moreover, as Wiśniewski (2018) and Silva (2020) suggest, freelance actors require investigative methods that extend beyond traditional group-based surveillance. France's early-warning architecture integrates these dimensions through its legal, technological and community-based mechanisms.

Legally, France has enacted a series of exceptional measures, including administrative searches, house arrests, expanded surveillance powers and the use of algorithmic tools for digital screening, as per the 2017 anti-terrorism law. While these powers provide investigative

agility, they also raise important concerns about civil liberties (Olech, 2022b). Nevertheless, they reflect a deliberate choice in favour of a pre-emptive, intelligence-led model of policing which, according to the EU Counter-Terrorism Agenda (CEU, 2005), is indispensable when dealing with rapidly radicalised individuals.

In the technological sphere, AI tools are employed by the DGSI and other agencies to detect anomalous behavioural patterns in digital environments, monitor extremist discourse on encrypted platforms, and support predictive modelling. These efforts echo for algorithm-enhanced counter-terrorism, while also requiring careful ethical regulation, particularly in avoiding bias and ensuring transparency in automated systems.

Furthermore, France's *Vigipirate Plan* plays a crucial role by integrating civil society into the detection process. Local partnerships involving police, educators and healthcare professionals are empowered to identify early signs of ideological shift, providing valuable HUMINT for central analysis. This model of decentralised vigilance, as emphasised in Part I, enhances the state's capacity to detect threats before they manifest violently.

In summary, the investigation of Freelance Terrorism in France is shaped by four interlinked pillars: (1) centralised intelligence coordination; (2) expansive legal authority; (3) technological innovation; and (4) community-based early detection. Despite the criticisms levelled against the potential for rights erosion, France's approach provides a structured and responsive model for navigating the complexities of decentralised terrorism in a high-risk environment.

DQ4: How can Freelance Terrorism be best prevented in Portugal? Preventing Freelance Terrorism in Portugal requires a multi-tiered strategy grounded in anticipatory intelligence, institutional articulation and societal resilience. Although Portugal has not experienced terrorist attacks attributed to freelance actors, the combination of structural vulnerabilities and evolving radicalisation dynamics demands proactive and context-sensitive measures.

The interviewees from IG Type A emphasised diverse but complementary preventive approaches. E1 highlighted the overarching role of the ENCT as the strategic umbrella guiding prevention. E2 focused on the importance of monitoring online environments and social dynamics, while E3 underscored awareness campaigns, OSINT, and training efforts aimed particularly at front-line units. However, the empirical data revealed some asymmetries in institutional investment in prevention, with E3 contributing the majority of coded references (67%), suggesting a more proactive operational stance.

From a theoretical standpoint, the Portuguese approach aligns with the principles of early-stage detection and decentralised vigilance discussed by Silva (2020) and Cortez (2021), who advocate for the integration of local actors and digital diagnostics in terrorism prevention. Furthermore, it's highlighted the importance of multi-level governance, where prevention is not solely the responsibility of intelligence services but shared among civil society, educational institutions and local authorities.

Nevertheless, one of the critical challenges identified by the interviewees was the early identification of radicalisation processes in the absence of structured networks (codes 12.1, 3.1, 3.2, 3.3, 3.4). This reflects a broader difficulty in applying conventional indicators to freelance profiles, whose motivations and trajectories are often opaque. Respondents called for enhanced digital literacy, youth engagement, and inter-institutional training, which are supported by the literature on community-based prevention (Silva, 2020; Cortez, 2021). The inclusion of civil society actors and the academic sector, as highlighted in responses to Question 19, reinforces the necessity of a whole-of-society approach.

Moreover, international coordination mechanisms, such as participation in Europol, the Counter Terrorism Group, and the TE-SAT reports, were cited by E2 and E3 as crucial in maintaining situational awareness and preventing the spillover of transnational radicalisation trends (codes 8.1, 9.1). These findings are consistent with the EU Counter-Terrorism Agenda (CEU, 2005), which stresses the interdependence of Member States in addressing emerging terrorist phenomena.

Although Portugal benefits from relative insulation, the absence of incidents may lead to complacency, a concern voiced by the interviewees. Thus, prevention must not be reactive but anticipatory and iterative, evolving in step with new digital threats and ideological patterns. As suggested by Olech (2022a), strategies must include behavioural analysis, algorithmic tools, and cross-sector education to counter freelance threats effectively.

In conclusion, the prevention of Freelance Terrorism in Portugal should not rely solely on institutional preparedness but must be rooted in a comprehensive prevention ecosystem, integrating strategic guidance (e.g., ENCT, 2023), operational training, digital awareness, and civil engagement. Reinforcing the role of the UCAT as a central coordination institution, while broadening cooperation with civil society and international platforms, will be key to enhancing Portugal's preventive capacity in the face of an unpredictable and decentralised threat landscape.

DQ5: How can Freelance Terrorism be best prevented in Poland? Preventing Freelance Terrorism in Poland requires a forward-looking strategy that integrates anticipatory intelligence, community engagement, and legislative readiness. Despite the absence of recorded attacks attributed to freelance actors, Polish authorities recognise the rising relevance of this threat due to transnational radicalisation trends, encrypted online environments, and geopolitical proximity to conflict-prone regions.

From the empirical data, both interviewees highlighted the centrality of early detection as a preventive pillar (codes 3.1, 3.3, 12.1). E5, in particular, underscored the need to track digital footprints, behavioural anomalies, and ideological indicators among vulnerable individuals. These findings align with the theoretical contributions of Cortez (2021) and Zubrzycki (2017), who argue that freelance radicalisation often manifests subtly within online or community settings, bypassing traditional surveillance systems.

A distinctive strength of the Polish model lies in its integrated operational posture, where elite tactical units do not merely execute reactive missions but also engage in upstream preventive measures. This dual role is exemplified by E5's emphasis on intelligence-led policing, public awareness campaigns, and scenario-based simulations (codes 5.2, 6.2, 18.2). Such activities reflect what Silva (2020) terms a "preventive intelligence ethos", which privileges pre-emptive situational modelling over classic surveillance.

Moreover, inter-agency coordination emerged as a significant enabling factor (codes 7.1, 7.2). Poland's counter-terrorism architecture benefits from close collaboration between the ABW, special police units, and local structures. Notably, the TPCE, operating under ABW, plays a pivotal role in bridging research, operational doctrine, and training. The TPCE integrates behavioural science, digital forensics, and community resilience building, which enhances preventive capacity, particularly against decentralised threats (TPCE, 2025; TPCE, 2021).

Another decisive factor is the robustness of the Polish legal framework, widely recognised as one of the most advanced in Europe (Wysocka, 2023). Polish legislation enables proactive measures, such as pre-emptive surveillance, digital monitoring and data retention policies, all while operating within the bounds of democratic oversight. Nonetheless, E5 advocated for continued legal adaptation, especially in light of AI deployment, privacy concerns and encrypted communications (codes 11.2, 15.11, 15.2), echoing the need for constant balance between security and civil liberties (Olech, 2022b).

Poland's geopolitical positioning also makes it a frontline state in detecting and preventing freelance terrorist infiltration via irregular migration or hybrid threat vectors. E5's

comments on refugee flows and border destabilisation (code 3.5) point to the importance of embedding prevention within multi-scalar frameworks, as argued by Puacz-Olszewska (2019). This calls for synchronised action across national and EU levels, particularly with Frontex and Europol (code 8.1).

Finally, the Polish approach includes community-focused measures, such as training local stakeholders to detect signs of radicalisation (codes 13.1, 13.2, 18.2, 18.3), indicating a shift toward relational intelligence. E5 noted the importance of trust-building between police and communities, a perspective aligned with Wiśniewski (2018) on grassroots prevention and the necessity of civil society as an intelligence multiplier.

In summary, the prevention of Freelance Terrorism in Poland is anchored in a hybrid model combining anticipatory intelligence, legal preparedness, operational integration and civic engagement. The presence of TPCE, the institutionalisation of community-based early warning, and an adaptive legal-infrastructural ecosystem position Poland as a reference point within the EU for preventing decentralised terrorist threats.

DQ6 How can Freelance Terrorism be best prevented in France? Preventing Freelance Terrorism in France involves a layered approach that combines national vigilance, institutional coordination and community engagement, anchored in a legislative and operational framework designed for pre-emptive action. France's long-standing exposure to terrorist threats, particularly after the 2015 attacks, has led to the development of one of the most structured and multidimensional counterterrorism architectures in Europe.

Central to this architecture is the *Plan Vigipirate*, a national framework that articulates graduated alert levels and mobilises a coordinated security response across civilian and military institutions (SGDSN, 2016). *Vigipirate* functions as both a preventive and communicational mechanism, enabling rapid adaptation of security measures in public spaces, transport hubs, and critical infrastructures (SGDSN, 2016). Its flexibility is particularly suited to decentralised threats, such as those posed by freelance actors who often seek soft, symbolic targets.

Complementing *Vigipirate* is the *Opération Sentinelle*, a permanent military deployment in urban areas launched after the *Charlie Hebdo* and *Bataclan* attacks. *Sentinelle* deploys thousands of armed soldiers across high-risk zones to deter opportunistic attacks and reinforce visible security. As noted in Part I, this military-civil interface acts as both a tactical deterrent and a public reassurance tool, enhancing the perception of state readiness and potentially dissuading radicalised individuals from acting (SGDSN, 2016).

At the institutional level, France maintains strong vertical and horizontal coordination between intelligence (DGSI), local authorities (PN and GN), judicial bodies and law enforcement. This synergy allows for swift identification of radicalised individuals through tools such as the FSPRT, which records behavioural signs of radicalisation even in the absence of criminal activity. This reflects the anticipatory logic advocated by Silva (2020), Olech (2022a) and Cortez (2021), positioning France at the forefront of behavioural intelligence-led prevention.

From a legal standpoint, the 2017 anti-terrorism law consolidated emergency powers into ordinary law, enabling administrative searches, house arrests and expanded video surveillance. While effective in targeting freelance threats at an early stage, these measures have raised concerns about civil liberties and the risk of stigmatisation. As Olech (2022b) points out, France's model represents a "security first" paradigm that prioritises preventive capacity, even at the expense of procedural guarantees.

Technology plays an increasingly central role. French authorities use artificial intelligence to monitor encrypted platforms, track radical discourse, and identify behavioural patterns across social media (CEU, 2005; Olech, 2022a). While this enhances preventive reach, it also raises ethical and technical challenges, particularly regarding data privacy and algorithmic bias.

In conclusion, France's approach to preventing Freelance Terrorism is built on a multi-layered infrastructure, where *Plan Vigipirate* and *Opération Sentinelle* form the operational backbone, supported by legal tools, behavioural detection and community engagement. Despite ongoing tensions between security and liberty, France offers a model of proactive and integrated prevention suited to the complex and evolving nature of decentralised terrorist threats.

In conclusion, in response to the Central Research Question – "**How can Freelance Terrorism be best prevented and countered in Portugal, based on the case studies of Poland and France?**" – the findings indicate that while Portugal's current framework provides a robust initial structure, significant adjustments are required to address the unique challenges posed by decentralised terrorist actors. Drawing on the Polish model's emphasis on anticipatory intelligence, community-based early detection and legal robustness, and on the French experience of centralised coordination, technological innovation and layered civil-military engagement, Portugal must transition toward a more proactive and integrated counter-terrorism strategy.

Specifically, the revision of the existing anti-terrorism legislation (Law n.º 52/2003) is critical, particularly in areas related to encrypted communications, the interception of involving communications and the recalibration of penalties for terrorism-related offences. Additionally, the development of a national early-warning and behavioural research centre would enhance the capacity for early detection of radicalisation trajectories, supported by investment in OSINT, HUMINT and AI-driven predictive risk models, with appropriate ethical oversight, in addition to TRAP-18 and HCR-20 v3 methodologies. Moreover, expanding targeted and continuous training for frontline operatives, especially in digital literacy and behavioural analysis, is essential to bridging current operational gaps. Formalising academic partnerships for secure threat modelling and integrating civil society actors into prevention frameworks would foster a whole-of-society approach. Finally, strengthening bilateral and multilateral cooperation mechanisms with EU security platforms, notably Europol and the Counter Terrorism Group, would consolidate Portugal's position within the European counter-terrorism ecosystem, ensuring alignment with best practices in confronting freelance terrorism.

CONCLUSION

This dissertation set out to investigate the optimal strategies for preventing and countering Freelance Terrorism in Portugal, drawing comparative insights from the case studies of Poland and France. The phenomenon of Freelance Terrorism, defined as ideologically motivated violence perpetrated by individuals or loosely organised micro-cells without formal ties to terrorist organisations, has emerged as one of the most elusive and unpredictable threats in the contemporary security landscape. Rooted in online radicalisation, sociopolitical grievances and digital autonomy, these actors challenge traditional counterterrorism frameworks that rely on organisational mapping and network disruption.

The study offers a pioneering comparative approach that integrates empirical fieldwork with theoretical reflection across three EU countries, filling a persistent gap in the literature regarding decentralised terrorism, in particular Freelance Terrorism. Through a multi-method research design combining theoretical analysis, comparative institutional study and empirical interviews with national experts, this work has produced a number of important findings. The Portuguese response to Freelance Terrorism, while normatively aligned with EU priorities and legally adequate in broad terms, remains fragmented and reactive. Interviews with national actors revealed institutional silos, limited operational preparedness and insufficient integration of digital behavioural intelligence into preventive practices. Conversely, Poland displayed a more cohesive and anticipatory model, particularly through the role of elite units and the TPCE, which promotes research, behavioural detection and early-warning mechanisms. France, despite the absence of direct interviews, was analysed through robust secondary sources and demonstrated a highly centralised and technologically sophisticated architecture, albeit one that raises concerns over civil liberties.

The key added value of this dissertation lies in the nuanced articulation of how these different national models can inform improvements to the Portuguese approach. It is now clear that Portugal would benefit from reinforcing its legal framework in specific areas, particularly with regard to the ethical use of metadata, behavioural monitoring and the digital traceability of radicalised individuals. The empirical findings reveal a partial mismatch between theoretical models of anticipatory intelligence ant their practical implementation in Portugal, where legal and institutional constraints limit proactive investigation. The creation of new legal mechanisms that allow for early and proportionate surveillance, including the ethical use of metadata, real-time digital monitoring and the operational deployment of preventive intelligence measures is

needed. It can be proposed, for instance, that the current legal framework should permit targeted vehicle searchers and home entries without prior judicial authorisation in cases of imminent threat, provided that they are subject to rapid judicial oversight (as it happened in Poland and France). Modern terrorism requires modern legal instruments, ones that balance constitutional protections with the capacity to prevent.

Furthermore, it's argued that traditional criminal law is inadequate for dealing with decentralised terrorist threats, calling instead for a preventive and proportionally grounded legislative approach that anticipates rather than reacts. This includes revising Portugal's antiterrorism law (Law n.º 52/2003), clarifying the legal definition of terrorism and expanding the authorised use of digital surveillance tools, including intercepting encrypted communications and applying ideological profiling to detect radicalisation pathways. He also stresses the need for better integration with EU norms, particularly concerning data interoperability. The comparative dimension also highlighted the potential for enhanced inter-institutional collaboration, not only between security services but also with academia. While operational secrecy is inevitable, the systematic and anonymised sharing of classified data for academic purposes, under appropriate safeguards, could substantially enrich national threat modelling and policy design.

The investigation also revealed several limitations and difficulties encountered during the research. Chief among them was the lack of empirical collaboration from French institutions, who initially agreed to participate but later withdrew without justification. Portuguese entities such as the PJ and OSCOT also failed to cooperate. The bureaucratic hurdles involved in obtaining official authorisations, as well as the scarcity of detailed, accessible reports on the subject, further constrained the research scope. The persistent reluctance of Portuguese institutions to engage with academic research not only restricts data availability but also signals a missed opportunity for evidence-based policymaking in counterterrorism. These obstacles reflect a broader culture of institutional opacity that continues to undermine the development of evidence-based counterterrorism policies.

Despite these limitations, the study contributes original insights and practical recommendations. From an operational standpoint, Portugal should consider establishing a dedicated research and early-warning centre akin to the TPCE, integrating psychological profiling, OSINT, HUMINT and strategic foresight. Moreover, the institutional articulation of prevention mechanisms must be expanded to include not only intelligence and policing actors

but also frontline staff (e. g. educators, local authorities) and civil society as a whole. Investment in digital literacy and community resilience is also paramount.

Future research could benefit from authorised access to restricted operational data, enabling longitudinal and mixed-method analyses that better capture the evolving nature of Freelance Terrorism, or Terrorism in general. Thus, it could be explored the longitudinal evolution of radicalisation trajectories in Portugal, the effectiveness of AI in counterterrorism intelligence, or the impact of national threat perception on institutional design. Additionally, it would be valuable to conduct comparative studies that incorporate non-EU actors or examine transnational terrorist financing networks, themes which, although relevant, fell outside the scope of the present work.

In practical terms, the study underscores the need for a hybrid counterterrorism strategy in Portugal, one that combines legal reform, anticipatory intelligence, multi-level cooperation and community-based resilience. This integrated approach is crucial for addressing the asymmetrical, diffuse and rapidly evolving nature of Freelance Terrorism. Ultimately, preventing and countering Freelance Terrorism in Portugal requires a shift from declarative strategy to operational integration. Lessons drawn from Poland and France reveal that legal adaptability, anticipatory intelligence and multi-level cooperation are not optional, bur essential.

In conclusion, this dissertation has demonstrated that Freelance Terrorism, as a decentralised and unpredictable threat, demands more than conventional counterterrorism paradigms. By drawing on comparative insights from Poland and France, it becomes evident that Portugal must transcend its reactive posture and move towards a proactive, technologically integrated and legally adaptive framework. A hybrid model that combines legal reform, anticipatory intelligence, operational coordination and civic resilience is not merely advisable but imperative. Only through the systematic integration of these dimensions can Portugal ensure the development of a counterterrorism strategy that is not only capable of addressing current threats but also resilient to the challenges of an evolving and increasingly complex security environment. This study thus offers a contribution to the broader academic and policy debates on decentralised terrorism, providing both a theoretical foundation and practical pathways for enhancing national security in the face of emerging threats. In so doing, it hopes to pave the way for a more robust and future-proof counterterrorism policy in Portugal.

REFERENCES

Academia Militar. (2024). *Normas para a redação de Trabalhos Finais de Investigação na Academia Militar*.

ACT of 6 April 1990 on the Police (1990). *Police* Act. Retrieved May 28, 2025, from https://www.policja.pl/ftp/pliki/police_act.pdf

Action Counters Terrorism. (2025). *Prevent Radicalisation and Extremism by Acting Early*. Retrieved May 28, 2025, from https://actearly.uk/

Agência da União Europeia para a Cooperação Policial [EUROPOL]. (2023). *TE-SAT 2023: European Union Terrorism Situation and Trend Report*. Retrieved May 28, 2025, from https://doi.org/10.2813/302117

Assembleia Geral das Nações Unidas [AGNU]. (1994). *Declaration on measures to eliminate international terrorism: Report of the Sixth Committee (A/49/743)*.

Bakker, E., & Graaf, B. de. (2010). *Lone Wolves: How to Prevent This Phenomenon?*

Baptista, C. S., & Sousa, M. J. (2011). *Como fazer investigação, dissertações, teses e relatórios segundo Bolonha* (4th ed.). Pactor.

Breivik, A. B. (2011). *2083 - A European declaration of independence: A manifesto*.

British Broadcasting Corporation [BBC]. (2011, July 24). *"Breivik manifesto" details chilling attack preparation*. Retrieved May 28, 2025, from https://www.bbc.com/news/world-europe-14267007

Campos, R. J. A. M. de. (2021). *O papel das Forças e Serviços de Segurança na deteção e Prevenção da ameaça terrorista em território português* [Master's Thesis, Military Academy].

Chancellery of the Prime Minister of the Republic of Poland. (2025). *Special Services*. Retrieved May 28, 2025, from https://www.gov.pl/web/special-services/about-us2#:~:text=DEPARTMENT%20OF%20NATIONAL%20SECURITY%20%28DBN%29%20is%20an%20organizational,of%20the%20Minister%20-%20Coordinator%20of%20special%20services.

Charmaz, K. (2004). Premises, Principles, and Practices in Qualitative Research: Revisiting the Foundations. *Qualitative Health Research*, *14*(7), 976–993. Retrieved May 28, 2025, from https://doi.org/10.1177/1049732304266795

Code pénal. (2022). *Version consolidée au 26 janvier 2022*. Retrieved May 28, 2025, from https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2022-01-26/

Combs, C. C., & Slann, M. (2007). *Encyclopedia of terrorism* (Rev. Ed.). Facts on File.

Committee of Ministers. (2018). *Council of Europe Counter-Terrorism Strategy (2018-2022)*. Retrieved May 28, 2025, from https://op.europa.eu/en/publication-detail/-/publication/292fd37c-30d8-11e9-8d04-01aa75ed71a1/language-pt#:~:text=Quer%20saber%20o%20que%20a%20UE%20alcan%C3%A7ou%20em,que%20a%20Uni%C3%A3o%20trouxe%20aos%20cidad%C3%A3os%20da%20UE%3F

Conselho da União Europeia. (2025). *A resposta da UE ao terrorismo*. Retrieved May 28, 2025, from https://www.consilium.europa.eu/pt/policies/fight-against-terrorism/

Constituição da República Portuguesa [CRP]. (1976). *Constituição da República Portuguesa*.

Cortez, F. (2021). *Contra-Terrorismo: Tópicos essenciais e a Unidade CT "ideal"* (1st ed.). Diário de Bordo.

Costa, C. S. F. (2016). *O Impacto do Terrorismo na Administração Interna em Portugal, no Século XXI*. [Master's Thesis, University of Lisbon].

Council Decision 2008/617/JHA (2008). *Concerning the Improvement of Cooperation between the Special Intervention Units of the Member States of the European Union in Crisis Situations*.

Council of Europe Committee on Counter-Terrorism [CDCT]. (2023). *Council of Europe Counter-Terrorism Strategy (2023-2027)*. Retrieved May 28, 2025, from https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680a9ad67%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

Council of the European Union [CEU]. (2005). *Estratégia Antiterrorista da União Europeia*. Retrieved May 28, 2025, from https://data.consilium.europa.eu/doc/document/ST%2014469%202005%20REV%204/PT/pdf

Decreto Lei n.º 78/1987, de 17 de fevereiro. (1987). *Código de Processo Penal*. Retrieved May 28, 2025, from https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis

Decreto Regulamentar n.º 2/2016, de 23 de agosto. (2016). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/decreto-regulamentar/2-2016-75170440

Decreto Regulamentar n.º 2/2016, de 23 de agosto. (2016). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/decreto-regulamentar/2-2016-75170440

Decreto-Lei n.º 275-A/2000, de 9 de setembro. (2000). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2000-70915729

Despacho Conjunto n.º 386/2006, de 9 de maio. (2006). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/despacho-conjunto/386-2006-2641669

Direction Générale de la Sécurité Intérieure [DGSI]. (2024, November 16). *Le fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)*. Retrieved May 28, 2025, from https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents/fichier-de-traitement

Douglas, K. S., Hart, S. D., Webster, C. D., Belfrage, H., Guy, L. S., & Wilson, C. M. (2014). Historical-Clinical-Risk Management-20, Version 3 (HCR-20 V3): Development and Overview. *International Journal of Forensic Mental Health*, *13*(2), 93–108. Retrieved May 28, 2025, from https://doi.org/10.1080/14999013.2014.906519

Duarte, F. P. (2013). 'Jihadismo de natureza autóctone' e 'lobos solitários' - a terceira forma de al-Qaeda. *Janus*, *20*(1), 48–49.

Esmailzadeh, Y. (2023). *An Introduction to Terrorism and Counter-Terrorism*. Retrieved May 28, 2025, from https://www.researchgate.net/publication/375085681

Estado Maior-General das Forças Armadas [EMGFA]. (2025). *Centro de Informações e Segurança Militares*. Retrieved May 28, 2025, from https://www.emgfa.gov.pt/pt/unidades/CISMIL

European Commission. (2020). *EU Security Union Strategy 2020-2025*. Retrieved May 28, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0605

European Council. (2004). *Declaração sobre a luta contra o terrorismo*.

European Gendarmerie Force [EUROGENDFOR]. (2025). *Żandarmeria Wojskowa – Member State*. Retrieved May 28, 2025, from https://eurogendfor.org/zandarmeria-wojskowa-full-member/

European Parliament. (2021, November 30). *Extending cooperation in the ATLAS network*. Retrieved May 28, 2025, from https://www.europarl.europa.eu/doceo/document/E-9-2021-005322_EN.html

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2014). *TE-SAT 2014: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2015). *TE-SAT 2015: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2016). *TE-SAT 2016: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2017). *TE-SAT 2017: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2018). *TE-SAT 2018: European Union Terrorism Situation and Trend Report*. Europol.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2019). *TE-SAT 2019: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2020). *TE-SAT 2021: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2021). *TE-SAT 2021: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2022). *TE-SAT 2022: European Union Terrorism Situation and Trend Report*.

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2023). *TE-SAT 2023: European Union Terrorism Situation and Trend Report*. Retrieved May 28, 2025, from https://doi.org/10.2813/302117

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2024). *TE-SAT 2024: European Union Terrorism Situation and Trend Report*. Retrieved May 28, 2025, from https://doi.org/10.2813/4435152

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2025a). *EU Internet Referral Unit - EU IRU*. Retrieved May 28, 2025, from https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru

European Union Agency for Law Enforcement Cooperation [EUROPOL]. (2025b). *European Counter Terrorism Centre - ECTC*. Retrieved May 28, 2025, from

https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc

Faluyi, O. T., Akinola, A. O., & Khan, S. (2019). Boko Haram's Terrorism and the Negerian State: Federalism, Politics and Policies. In *Advances in African Economic, Social and Political Development*. Springer. Retrieved May 28, 2025, from https://doi.org/https://doi.org/10.1007/978-3-030-05737-4

Faustino, P. A. T. (2018). *Terrorismo Jihadista em França: Da Segurança ao Securitarismo*. [Master's Thesis, Economy Faculty of the University of Coimbra].

Federal Bureau of Investigation [FBI]. (2025). *Terrorism*. Retrieved May 28, 2025, from https://www.fbi.gov/investigate/terrorism

Fortin, M. F. (1999). *O Processo de Investigação: Da concepção à realização*. LusoCiência.

Freixo, M. J. V. (2011). *Metodologia Científica: Fundamento, Métodos e Técnicas*. Instituto Piaget.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2014). *Relatório Anual de Segurança Interna 2014*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2015). *Relatório Anual de Segurança Interna 2015*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2016). *Relatório Anual de Segurança Interna 2016*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2017). *Relatório Anual de Segurança Interna 2017*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2018). *Relatório Anual de Segurança Interna 2018*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2019). *Relatório Anual de Segurança Interna 2019*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2020). *Relatório Anual de Segurança Interna 2020*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2021). *Relatório Anual de Segurança Interna 2021*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2022). *Relatório Anual de Segurança Interna 2022*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2023). *Relatório Anual de Segurança Interna 2023*.

Gabinete do Secretário-Geral do Sistema de Segurança Interna [GSGSSI]. (2024). *Relatório Anual de Segurança Interna 2024*.

Ganor, B. (2015). *Global Alert: The Rationality of Modern Islamist Terrorism and the Challenge to the Liberal Democratic World*. Columbia University Press.

Gartenstein-Ross, D., Barr, N., & Moreng, B. (2016). *The Islamic State's Global Propaganda Strategy*. International Centre for Counter-Terrorism. Retrieved May 28, 2025, from https://doi.org/10.19165/2016.1.01

Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Social* (6th ed.). Atlas.

Godinho, M. J., & Pereira, F. (2019). *Exercício pelas forças armadas de funções de segurança interna em tempo de paz*.

Gouvernement Français. (2006). *Livre blanc sur la sécurité intérieure face au terrorisme*.

Guarda Nacional Republicana [GNR]. (2025). *Comandos e Unidades*. https://www.gnr.pt/unidades.aspx

Guerra, I. C. (2006). *Pesquisa Qualitativa e Análise de Conteúdo: Sentidos e Formas de Uso*. Principia.

Henne, P. (2019, January 25). Terrorism and Religion: An Overview. *Oxford Research Encyclopedia of Politics*. Retrieved May 28, 2025, from https://doi.org/10.1093/acrefore/9780190228637.013.693

Institute for Economics & Peace. (2014). *Global Terrorism Index 2014: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2015). *Global Terrorism Index 2015: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2016). *Global Terrorism Index 2016: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2017). *Global Terrorism Index 2017: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2018). *Global Terrorism Index 2018: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2019). *Global Terrorism Index 2019: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2020). *Global Terrorism Index 2020: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2021). *Global Terrorism Index 2021: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2022). *Global Terrorism Index 2022: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2023). *Global Terrorism Index 2023: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2024). *Global Terrorism Index 2024: Measuring the impact of terrorism*.

Institute for Economics & Peace. (2025a). *Evolving Patterns of Terrorism & Radicalisation in Western Democracies: Lone Wolf and Youth Terrorism*. www.economicsandpeace.org

Institute for Economics & Peace. (2025b). *Global Terrorism Index 2025: Measuring the impact of terrorism*.

Internal Security Agency [ABW]. (2025). *The Internal Security Agency*. Retrieved May 28, 2025, from https://www.abw.gov.pl/en

Johnson, R. B., & Christensen, L. (2014). *Educational Research: Quantitative, Qualitative, and Mixed Approaches* (5th ed.). Sage.

Kochańczyk, R. (2020). Counter Terrorism Strategy. *Zeszyty Naukowe*, *1*(73), 242–258. Retrieved May 28, 2025, from https://doi.org/10.5604/01.3001.0014.0783

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). New Age International Publishers.

Leandro, G. (2004). Uma visão militar sobre o terrorismo. In A. Moreira, *Terrorismo* (2nd ed., pp. 525–533). Almedina.

Lei n.º 9/2007, de 19 de fevereiro. (2007). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/lei/9-2007-517985

Lei n.º 30/84, de 5 de setembro. (1984). Retrieved May 28, 2025, from https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=764&tabela=leis&so_miolo=

Lei n.º 49/2008, de 27 de agosto. (2008). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/lei/49-2008-453255

Lei n.º 52/2003, de 22 de agosto. (2003). Retrieved May 28, 2025, from https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=119&tabela=leis

Lei n.º 53/2007, de 31 de agosto. (2007). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-174279072-174332731

Lei n.º 53/2008, de 29 de agosto. (2008). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-34501675

Lei n.º 63/2007, de 6 de novembro. (2007). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/lei/63-2007-629449

Lei n.º 83/2017, de 18 de agosto. (2017). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/lei/83-2017-108021178

Lippay, C. (2021). *The ATLAS Network: European Special Intervention Units combating terrorism and violent crime*. Stumpf + Kossendey Verlag.

Loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme. (1986). Retrieved May 28, 2025, from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000693912

Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. (2017). Retrieved May 28, 2025, from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000035932811/2021-02-06/

Lopes, J. A. (2019). Definição e Resposta ao Terrorismo na UE e em Portugal: o Que Fazer das Mulheres e Crianças Afiliadas ao Daesh? *Nação e Defesa*, *154*, 109–144.

Marconi, M. de A., & Lakatos, E. M. (2003). *Fundamento de Metodologia Científica* (5th ed.). Atlas.

Meloy. (2021). *Terrorist Radicalization Assessment Protocol-18 (TRAP-18)*.

Meggitt, J. J. (2020). In Response-Does religion cause terrorism? The problem of religion and the need for a better question. *Contemporary Voices, 1*(1), 66–72. Retrieved May 28, 2025, from https://doi.org/10.15664/jtr.1601/

Military Counterintelligence Service [SKW]. (2025). *Military Counterintelligence Service*. Retrieved May 28, 2025, from https://www.skw.gov.pl/en/index.html

Military Intelligence Service [SWW]. (2025). *Military Intelligence Service*. Retrieved May 28, 2025, from https://www.sww.gov.pl/en/

Ministère de la Justice [MJ]. (2019, September 30). *Zoom sur le nouveau Parquet national antiterroriste*. Retrieved May 28, 2025, from

https://www.justice.gouv.fr/actualites/actualite/zoom-nouveau-parquet-national-antiterroriste

Ministère de l'Économie, des F. et de la S. industrielle et numérique [ME]. (2025a). *La Direction Nationale du Renseignement et des Enquêtes Douanières*. Retrieved May 28, 2025, from https://www.douane.gouv.fr/fiche/la-direction-nationale-du-renseignement-et-des-enquetes-douanieres

Ministère de l'Économie, des F. et de la S. industrielle et numérique [ME]. (2025b). *Tracfin - Service de renseignement financier*. Retrieved May 28, 2025, from https://www.economie.gouv.fr/tracfin

Ministère de l'Intérieur [MIA]. (2025a). *Direction Générale de la Sécurité Intérieure*. Retrieved May 28, 2025, from https://www.dgsi.interieur.gouv.fr/

Ministère de l'Intérieur [MIA]. (2025b). *Police Nationale*. Retrieved May 28, 2025, from https://www.police-nationale.interieur.gouv.fr/nous-decouvrir/notre-organisation/organisation/direction-nationale-de-police-judiciaire-dnpj

Ministère de l'Intérieure [MIA]. (2024, November 26). *Les services judiciaires anti-terroristes*. Retrieved May 28, 2025, from https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/police-judiciaire-specialisee/services-judiciaires-anti-terroristes

Ministère des Armées [MND]. (2025a). *Direction du Renseignement et de la Sécurité de la Défense*. Retrieved May 28, 2025, from https://www.defense.gouv.fr/drsd

Ministère des Armées [MND]. (2025b). *Direction du Renseignement Militaire*. Retrieved May 28, 2025, from https://www.defense.gouv.fr/drm

Ministère des Armées [MND]. (2025c). *Direction Générale de la Sécurité Extérieure*. Retrieved May 28, 2025, from https://www.dgse.gouv.fr/fr

Ministério Público [MP]. (2025). *Departamento Central de Investigação e Ação Penal*. Retrieved May 28, 2025, from https://dciap.ministeriopublico.pt/

Ministerstwo Obrony Narodowej [MND]. (2023). *Jednostka Wojskowa Formoza*. Retrieved May 28, 2025, from https://formoza.wp.mil.pl/

Ministerswo Obrony Narodowej [MND]. (2025). *Jednostka Wojskowa GROM*. Retrieved May 28, 2025, from https://www.gov.pl/web/mswia/wojska-specjalne

National Consortium for the Study of Terrorism and Responses to Terrorism [START]. (2025). *Global Terrorism Database (GTD)*. Retrieved May 28, 2025, from https://www.start.umd.edu/data-tools/GTD

Nowopolski, M., Banasik, M., & Gierowski, J. K. (2018). Warning Behaviours and Risk Factors Preceding Acts of Individual Terrorism. *Problems of Forensic Sciences*, *116*, 323–338.

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 4 kwietnia 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o działaniach antyterrorystycznych. (2019). Retrieved May 28, 2025, from https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000796/T/D20190796L.pdf

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 maja 2024 r. w sprawie ogłoszenia jednolitego tekstu ustawy o Straży Granicznej. (2024). Retrieved May 28, 2025, from https://dziennikustaw.gov.pl/D2024000091501.pdf

Olech, A. (2021). *Counterterrorism Strategies in Poland and France*. Warsaw Institute. Retrieved May 28, 2025, from www.warsawinstitute.org

Olech, A. (2022a). *French and Polish Fight Against Terrorism*. Kontekst Publishing House.

Olech, A. (2022b). Legislation on Combating Terrorism in the Republic of Poland. In *Changing Global Security Architecture* (pp. 100–132). Proceedings XXI.

North Atlantic Treaty Organization [NATO]. (2020). *AAP-06: Nato glossary of terms and definitions (English and French).*

Organization for Security and Co-operation in Europe [OSCE]. (2014). *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach*.

Organization for Security and Co-operation in Europe (OSCE). (2014). *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach: Vol. I* (1st ed.). Organization for Security and Co-operation in Europe.

Pantucci, R. (2011). A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists. In *Developments in Radicalisation and Political Violence*. www.icsr.info

Parker, T., & Sitter, N. (2016). The Four Horsemen of Terrorism: It's Not Waves, It's Strains. *Terrorism and Political Violence*, *28*(2), 197–216. Retrieved May 28, 2025, from https://doi.org/10.1080/09546553.2015.1112277

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th ed.). Sage. Retrieved May 28, 2025, from

https://archive.org/details/michael-quinn-patton-qualitative-research-evaluation-methods-integrating-theory-/page/n3/mode/2up

Police Nationale [PN]. (2025a). *Le RAID: Recherche, Assistance, Intervention, Dissuasion*. Retrieved May 28, 2025, from https://www.police-nationale.net/raid/

Police Nationale [PN]. (2025b). *Les Brigades de Recherche et d'Intervention de la Police Nationale – Antigang*. Retrieved May 28, 2025, from https://www.police-nationale.net/bri/

Police Nationale [PN]. (2025c). *Les Compagnies Républicaines de Sécurité: missions, recrutement*. Retrieved May 28, 2025, from https://www.police-nationale.net/compagnies-republicaines-securite/

PoliceFR. (2025). *Le rôle de l'UCLAT : unité de coordination de la lutte antiterroriste*. Retrieved May 28, 2025, from https://www.policefr.com/uclat/

Polícia de Segurança Pública [PSP]. (2025). *Polícia de Segurança Pública*. Retrieved May 28, 2025, from https://www.psp.pt

Polícia Judiciária [PJ]. (2025). *Polícia Judiciária*. Retrieved May 28, 2025, from https://www.policiajudiciaria.pt/

Polish National Police [PP]. (2025a). *Centralny Pododdział Kontrterrorystyczny Policji "BOA"*. Retrieved May 28, 2025, from https://www.policja.pl/pol/boa/332,Centralny-Pododdzial-Kontrterrorystyczny-Policji-quotBOAquot.html

Polish National Police [PP]. (2025b). *Polish National Police*. Retrieved May 28, 2025, from https://www.policja.pl/pol/english-version/4889,Polish-National-Police.html

Prodanov, C. C., & Freitas, E. C. (2013). *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico* (2nd ed.). Universidade Feevale. Retrieved May 28, 2025, from www.feevale.br/editora

Puacz-Olszewska, J. (2019). Combating Terrorism in the European Union and the Republic of Poland. In *Modern Management Review 24*(1), pp. 71–81). Rzeszow University of Technology. Retrieved May 28, 2025, from http://mmr.prz.edu.pl/

Quivy, R., & Campenhoudt, L. Van. (2008). *Manual de Investigação em Ciências Sociais*. Gradiva.

Rapoport, D. C. (2013). The Four Waves of Modern Terror: International Dimensions and Consequences. In J. M. Hanhimäki & B. Blumenau, *An International History of Terrorism: Western and Non-Western Experiences* (pp. 282–310). Routledge.

Retrieved May 28, 2025, from https://doi.org/https://doi.org/10.4324/9780203093467

Reinares, F., & García-Calvo, C. (2013). *Significado y Alcance de la Yihad Terrorista Individual*.

Resende, R. (2016). Técnica de Investigação Qualitativa: ETCI. *Journal of Sport Pedagogy & Research*, *2*(1), 50–57.

Resolução do Conselho de Ministros n.º 7-A/2015. (2015). Retrieved May 28, 2025, from https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2525&tabela=leis&ficha=1

Resolução Do Conselho de Ministros n.º 40/2023, de 03 de maio. (2023). Retrieved May 28, 2025, from https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/40-2023-212551390

Rodrigues, A. L. (2021). Investigação - Ação e Análise de Conteúdo: Caso na Formação de Professores. *Práxis Educacional*, *17*(48), 1–23. Retrieved May 28, 2025, from https://doi.org/10.22481/praxisedu.v17i48.8796

Rosado, D. P. (2017). *Elementos Essenciais de Sociologia Geral*. Gradiva.

Rossmo, D. K. (2000). *Geographic Profiling*. CRC Press. Retrieved May 28, 2025, from https://api.pageplace.de/preview/DT0400.9781420048780_A41210520/preview-9781420048780_A41210520.pdf

Santos, L. A. B., & Lima, J. M. M. do V. (2019). Orientações metodológicas para a elaboração de trabalhos de investigação (2nd ed.). *Cadernos Do IUM*, *8*.

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses* (1st ed.). Universidade Lusíada Editora.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). Pearson.

Schmid, A. P. (2021). Handbook of Terrorism Prevention and Preparedness. In *Handbook of Terrorism Prevention and Preparedness*. International Centre for Counter-Terrorism. Retrieved May 28, 2025, from https://doi.org/10.19165/2020.6.01

Secrétariat Général de la Défense et de la Sécurité Nationale [SGDSN]. (2016). *Tackling Terrorism Together: Vigilance, Prevention, and Protection Against the Terrorist Threat - VIGIPIRATE*.

Serviço de Informações de Segurança [SIS]. (2024). *Serviço de Informações de Segurança*. Retrieved May 28, 2025, from https://www.sis.pt/

Serviço de Informações Estratégicas de Defesa [SIED]. (2025). *Serviço de Informações Estratégicas de Defesa*. Retrieved May 28, 2025, from https://www.sied.pt/

Silva, T. M. G. (2020). *Evitar Atentados Terroristas Freelance: Do profiling às medidas que faltam tomar*. Escrytos.

Silva, T. M. G. (2015). *A ameaça terrorista em Portugal*. [Doctorate's Thesis, New Lisbon University].

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, *21*(5), 619–634. Retrieved May 28, 2025, from https://doi.org/10.1080/13645579.2018.1454643

Sistema de Informações da República Portuguesa [SIRP]. (2025). *Sistema de Informações da República Portuguesa*. Retrieved May 28, 2025, from https://www.sirp.pt/

Spaaij, R. (2012). *Understanding Lone Wolf Terrorism*. Springer. Retrieved May 28, 2025, from https://doi.org/10.1007/978-94-007-2981-0

Terrorism Prevention Centre of Excellence [TPCE]. (2021). *Terrorism: Prevention Guide*. Agencja Bezpieczeństwa Wewnętrznego. Retrieved May 28, 2025, from www.tpcoe.gov.pl

Terrorism Prevention Centre of Excellence [TPCE]. (2025). *Terrorism Prevention Internal Security Agency*. Retrieved May 28, 2025, from https://www.tpcoe.gov.pl/cpe

The International Criminal Police Organization [INTERPOL]. (2025). *Terrorism*. https://www.interpol.int/en/Crimes/Terrorism

Touati, F. (2023). *Stratégies et mécanismes de lutte contre le terrorisme. Illustration par une étude comparative des expériences française et tunisienne.* [Doctorate's Thesis, Côte d'Azur University].

Troin, O. A., & Léonard, C. (2016). *Rapport d'information n.º 3864 - sur la présence et l'emploi des forces armées sur le territoire national*. Retrieved May 28, 2025, from https://www.assemblee-nationale.fr/dyn/14/rapports/cion_def/l14b3864_rapport-information

União Europeia [UE]. (2002). *Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo*. Retrieved May 28, 2025, from https://eur-lex.europa.eu/eli/dec_framw/2002/475/oj/eng#document1

União Europeia [UE]. (2017). Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui

a Decisão-Quadro 2002/475/JAI do Conselho e que altera a Decisão 2005/671/JAI do Conselho. In *Jornal Oficial da União Europeia*. Retrieved May 28, 2025, from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32017L0541

United Nations General Assembly [UNGA]. (1972). *Resolução 3034 (XXVII): Medidas para prevenir o terrorismo internacional que põe em perigo ou tira vidas humanas inocentes ou compromete as liberdades fundamentais*.

United Nations General Assembly [UNGA]. (1994). *Declaration on measures to eliminate international terrorism: Report of the Sixth Committee (A/49/743)*.

United Nations Office of Counter-Terrorism [UNOCT]. (2024). *United Nations Office of Counter-Terrorism*. https://www.un.org/counterterrorism/

United Nations Office on Drugs and Crime [UNODC]. (2018). *Counter-Terrorism 1: Introduction to International Terrorism*.

United Nations [UN]. (1945). *United Nations Letter*. www.ministeriopublico.pt

United Nations [UN]. (2025a). *United Nations Office of Counter-Terrorism*. Retrieved May 28, 2025, from https://www.un.org/counterterrorism/

United Nations [UN]. (2025b). *Universal Declaration of Human Rights*. Retrieved May 28, 2025, from https://www.ohchr.org/en/human-rights/universal-declaration/translations/english

University of Gdansk. (2024, January 8). *How to behave under a terrorist attack? 4U campaign*. Retrieved May 28, 2025, from https://ug.edu.pl/news/en/6317/how-behave-under-terrorist-attack-4u-campaign

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. (2002). Retrieved May 28, 2025, from https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20020740676/T/D20020676L.pdf

Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych. (2001). Retrieved May 28, 2025, from https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20011231353

Vilelas, J. (2020). *Investigação: O Processo de Construção do Conhecimento* (3rd ed.). Edições Sílabo.

Wiśniewski, B. (2018). The Polish Legal and Organisational Solutions Combating Terrorism. *Internal Security*, *10*(1), 137–145. Retrieved May 28, 2025, from https://doi.org/10.5604/01.3001.0012.7495

Wysocka, M. D. (2023). *Islamski terroryzm kobiet jako wyzwanie i zagrożenie dla bezpieczeństwa we współczesnym świecie*.

Yitzhak, E. (2013). *Síndrome de Yihad Súbito*.

Zięba, A. (2015). Counterterrorism Systems of Spain and Poland: Comparative Studies. *Przegląd Politologiczny*, *3*(15), 65–78. Retrieved May 28, 2025, from https://doi.org/10.14746/pp.2015.20.3.5

Zubrzycki, W. (2015). Combating Terrorism through Interdepartmental Projects. *Internal Security*, *1*(1), 104–121. Retrieved May 28, 2025, from https://doi.org/10.5604/20805268.1192773

Zubrzycki, W. (2017). Combating Terrorism in Republic of Poland. *Public Security and Public Order*, *1*(18), 77–90.

APPENDICES

APPENDIX A – THEORETICAL FRAMEWORK

Appendix A.1 – Historical and Conceptual Evolution of Terrorism

From the 19th century onwards, terrorism ceased to be limited to isolated political assassinations and evolved into a systematic method of ideological struggle. Throughout the 20th century, it adapted to shifting geopolitical contexts, from anti-colonial campaigns to ideological confrontations during the Cold War, becoming progressively transnational and more symbolic in nature.

A crucial conceptual distinction should be made between "terror", a general state of fear often produced by acts of violence, and "terrorism", which is defined by its intentional use of violence for ideological, political or religious goals and its symbolic communication strategy. As Schmid (2021) argues, terrorism does not aim merely to kill but to influence public opinion, intimidate populations and coerce institutions. Its targets, methods and messages are carefully chosen to provoke maximum psychological and political effect.

Additionally, another conceptual clarification relates to the distinction between antiterrorism and counterterrorism. While often used interchangeably, the former typically refers to preventive measures, whereas the latter concerns operational responses. As noted by Townshend (cited in Cortez, 2021), both dimensions are essential and in practice, interdependent in the design of modern security strategies. In the present study, however, both terms are regarded as equivalent, insofar as the fight against terrorism inevitably requires joint action in both spheres.

Appendix A.2 – Challenges in Achieving an International Definition of Terrorism

Despite widespread recognition of terrorism as a global threat, no single definition has achieved full international consensus. As outlined in the main text, this is due to political divergences, historical sensitivities, and the strategic implications of classification. The 1937 Convention for the Prevention and Punishment of Terrorism, promoted by the League of Nations, was the first notable attempt to establish a legal definition, introducing the concept of terrorism as a crime not only against individual states but also against the international community (UNODC, 2018).

The debate intensified in later decades, especially concerning the distinction between *"*terrorists*"* and *"*freedom fighters*"*, with the latter claiming legitimacy through the right to

self-determination (UN, 1945; UNODC, 2018). This tension emerged in several United Nations General Assembly (UNGA) resolutions:

- **Resolution 3034 (1972)**[52] called for greater understanding of the causes of violence (UNGA, 1972);
- **The 1994 Declaration on Measures to Eliminate International Terrorism affirmed** that all acts of terrorism must be unequivocally condemned as criminal and unjustifiable (UNGA, 1994)[53,54].

Several international and regional organisations have since adopted their own definitions:

- **NATO**: Terrorism is the unlawful use or threat of use of force to intimidate or coerce governments or societies for ideological, political or religious objectives (NATO, 2020)[55];
- **GTI**: Defines terrorism as "the systematic use of violence by non-state actors intended to send a political, religious, or ideological message, generate fear, and influence a broader audience" (Institute for Economics & Peace, 2023);
- **EU:**
  - **Directive 2017/541**[56] (replacing Framework Decision 2002/475/JHA): Defines terrorism as acts intended to "seriously intimidate a population, unduly compel a government or international organisation to perform or abstain from performing an act, or seriously destabilise political, economic or social structures" (EU, 2017);
  - **EU Counter-Terrorism Strategy (2005)**: Frames terrorism as a common threat to Member States and adopts a four-pillar approach: prevent, protect, pursue, and respond (CEU, 2025**;** EU, 2002);

[52] *Vide* paragraphs 2 and 5 of United Nations General Assembly Resolution 3034 (XXVII), of 18 December 1972.

[53] This condemnation is justified by the fact that the relationship between states and their populations is undermined, thereby threatening their peace, security, and integrity (UNGA, 1994).

[54] Report of the Sixth Committee of the United Nations, Item 142, Resolution 490, UNGA, Doc. A/49/743 (UNGA, 1994).

[55] This NATO definition has remained unchanged up to the most recent edition of publication AAP-6, issued in 2020.

[56] This amendment further strengthened European legislation concerning the criminalisation of terrorist acts and cooperation among Member States.

- **Latest EU legal interpretation (2025)**: Defines terrorist acts as those committed to "seriously intimidate a population, destabilise or destroy fundamental structures, or unduly compel a government to act or refrain from acting in a given domain" (CEU, 2025);

– **United States of America** (USA) with **FBI** (2025)[57]: Distinguishes between international terrorism (linked to foreign organisations) and domestic terrorism (inspired by internal ideologies, including political and religious extremism).

Despite these variations, most definitions share common elements: i) intentional use of violence, ii) driven by ideological/political aims at creating fear or coercing institutions. Nonetheless, the lack of full international consensus remains a significant barrier to unified action, especially in extradition, prosecution, and intelligence cooperation. As such, understanding the institutional landscape of definitions is essential for analysing national and international counter-terrorism strategies.

Appendix A.3 – Typologies of Terrorism

To complement the typological framework adopted in the core of this dissertation, this appendix offers a deeper exploration of alternative classifications and critical perspectives. While Rapoport's model of the "Four Waves of Modern Terrorism" has been introduced in the main text, it is worth noting that each wave corresponds to a specific historical and ideological context:

– The Anarchist Wave (late 19th century – 1920s): Marked by targeted violence against political leaders, exemplified by the assassination of Tsar Alexander II of Russia in 1881;

– The Anti-Colonial Wave (1920s – 1960s): Driven by national liberation movements resisting European colonial rule;

– The New Left Wave (1960s – end of the Cold War in 1989): A fusion of radical leftist ideologies and nationalist aspirations, often represented by groups like ETA;

[57] The FBI is one of the leading institutions in the USA responsible, *inter alia*, for combating both domestic and international terrorism.

- The Religious Wave (1990s – present): Characterised by violent actions inspired by religious fundamentalism, notably Al-Qaeda and Daesh, seeking to influence international politics (Ganor, 2015, p. 2).

The critiques raised by Parker and Sitter (2016), Combs and Slann (2007), and Esmailzadeh (2023), while already summarised in subchapter 1.3., underscore the need to consider terrorism as both ideologically persistent and strategically performative, rather than as a linear historical process. These insights support the use of flexible and multilayered typologies. Particularly useful in this regard is the typology proposed by Ventura & Dias (2015, cited in Cortez, 2021, p. 40-41), which distinguishes five ideological currents:

- Far-left and far-right terrorism: Far-left movements (inspired by Marxism–Leninism) aim to destroy capitalism and Western democratic regimes; Far-right groups often draw from fascist and national-socialist ideologies, opposing immigration and multiculturalism;
- Anarchist and anti-globalisation movements: Reject capitalist structures, liberal globalisation, and technocratic governance, often through direct action;
- Secessionist, separatist, and nationalist groups: Advocate for the independence of a specific geographic area, sometimes through ethnonationalist rhetoric or territorial claims;
- Eco-terrorism and radical activism: Centre their campaigns on the protection of the environment, animals, and minority groups, often attacking symbols of industrial development;
- Religiously inspired terrorism: Focused primarily on jihadist interpretations of Islam, with the goal of establishing theocratic regimes based on strict applications of Sharia law (Islamic law).

These typologies are not mutually exclusive and often intersect. Nonetheless, they provide valuable nuance for understanding the shifting motivations and methods of terrorist actors in a context increasingly marked by ideological hybridisation and operational decentralisation.

Appendix A.4 – Jihadist Terrorism

This appendix offers a complementary reflection on the doctrinal manipulation and adaptive capacity of jihadist terrorism, aspects briefly introduced in subchapter 1.4. One of

the defining features of contemporary jihadism[58,59] is its strategic exploitation of religious ambiguity to justify political violence. According to Cortez (2021), extremist groups skilfully manipulate sacred texts and theological interpretations, presenting violence as a divine duty, while simultaneously reinforcing their narratives through the miscommunication between Western and Islamic societies.

A central feature of jihadist terrorism is the manipulation of interpretative ambiguities within religious doctrine and the instrumental use of digital platforms, both to recruit sympathisers and to spread propaganda. According to Cortez (2021), such groups deliberately exploit cultural ignorance and miscommunication between Western and Islamic societies, reinforcing their narrative through both mainstream media (MSM) discourse and radical messaging. On one hand, certain media commentators and self-proclaimed experts contribute to misconceptions by disseminating sensationalist or reductive interpretations of Islam. On the other, jihadist organisations such as ISIS and Al-Qaeda weaponise these distortions to attract recruits and sustain ideological momentum (Schmid, 2021).

The adaptive nature of jihadism, including its ability to integrate decentralised actors such as freelance terrorists and lone wolfs, is central to its resilience. Both profiles share characteristics such as self-radicalisation, frequently in online ecosystems or prison environments and a capacity for high-impact symbolic violence with minimal operational footprint (Bakker & Graaf, 2010; Gartenstein-Ross *et al*., 2016; Schmid, 2021).

This operational flexibility, coupled with its symbolic and emotional appeal, renders jihadist terrorism particularly resistant to classical counterterrorism strategies. It demands, therefore, a combination of ideological contestation, community engagement, strategic communication and digital surveillance capable of challenging its foundational narratives while preserving democratic values.

[58] One of the most important concepts that is used inaccurately is Jihad, since it is presented as an incitement to violence. However, the current translations, "Holy War", can be misleading, since jihad literally means "endeavour" or "struggle". A struggle that is predominantly internal, in the sense of observing Islamic precepts, and its convolution into a literal war, against the "infidels". (Cortez, 2021)

[59] This form of terrorism has manifested itself in different historical and confessional contexts, including attacks committed by extremists from other religions (e.g. Christians), although Islamic Jihadism has taken on greater international expression due to its organisation, media visibility and geopolitical impact. (Meggitt, 2020)

APPENDIX B – DYNAMICS OF RADICALISATION AND INDIVIDUALISED TERRORISM

Appendix B.1 – Key Dynamics and Contemporary Trends in Radicalisation

Radicalisation does not follow a single, linear path, but rather unfolds through heterogeneous trajectories shaped by the interaction of individual, social, and ideological factors. While the core stages, polarisation, activism, extremism and terrorism, have been broadly identified (TPCE, 2021), their manifestation varies significantly across contexts and individuals.

Certain psychosocial drivers interact with each other to shape vulnerability to extremist messaging. These factors are often (TPCE, 2021):

- Individual socio-psychological factors: identity crises, feelings of marginalisation[60], perceptions of injustice or humiliation, belief in conspiracy theories, personal or collective victimisation;
- Social factors: exclusion[61], discrimination, lack of education, misinformation, and disinformation[62];
- Political factors: perceptions of cultural or civilisational tensions, nationalist or separatist aspirations, exposure to hate speech;
- Ideological/religious factors: belief in the superiority or victimisation of a faith or ideology, adherence to apocalyptic narratives, martyrdom;
- Cultural and identity-related factors: lack of cultural belonging, identity confusion, vulnerability to radical narratives;
- Trauma: early-life adversity, family dysfunction, or exposure to violence.

The process is often catalysed by three main dynamics (TPCE, 2021): i) Radicalisers: ideological influencers who exploit personal vulnerabilities and manipulate beliefs; ii) Group dynamics: collective reinforcement through charismatic leaders or peers offering

[60] Alternatively, marginalisation or self-marginalisation may result from the broader phenomenon of ghettoisation, whereby certain communities become spatially and socially segregated from mainstream society.
[61] In certain cases, self-exclusion or self-imposed social marginalisation among specific groups of individuals leads to the ghettoisation of entire communities.
[62] Social engineering, in this context, particularly when maliciously applied to exploit the human factor, broadens the spectrum of potential attacks, especially through the dissemination of disinformation and hate speech. When combined with OSINT (Open-Source Intelligence) techniques, this information may be deliberately manipulated and weaponised to facilitate or incite an attack.

identity and purpose; iii) Online ecosystems[63]: digital spaces enabling ideological dissemination, recruitment, and operational instruction. These enable the widespread dissemination of terrorist propaganda and allows for forms of virtual participation that facilitate both recruitment and the transmission of operational instructions.

Based on these dynamics, we can identify overlapping models (TPCE, 2021): i) Leader-led radicalisation, guided by charismatic mentors; ii) Group-based radicalisation, driven by peer influence and in-group validation; iii) Individual radicalisation, often occurring in digital isolation, sometimes leading to "lone wolf" or freelance terrorism.

Contemporary terrorism trends are also reshaping the radicalisation landscape. The most prominent developments include (TPCE, 2021):

- Online radicalisation and propaganda: increased use of social media for disseminating ideologies and recruiting followers;
- Freelance and lone actor terrorism: self-radicalised individuals who act independently, complicating detection and prevention;
- Technological innovation in attacks: use of cyber capabilities, biological, and chemical weapons has increased the lethality and unpredictability of terrorist activity;
- Balancing legality and security: the challenge of countering terrorism without undermining civil liberties;
- Youth radicalisation[64]: high exposure of younger populations to radical content online, increasing their susceptibility to extremist recruitment (Institute for Economics & Peace, 2025a).

These developments underscore the need for preventive strategies that combine resilience-building, digital literacy, early detection mechanisms, and cross-sectoral coordination.

[63] It is important to draw a distinction between "cyberterrorism" and the cyber dimension of terrorism. The former refers to disruptive or destructive acts targeting non-combatants, committed by or under the influence of terrorist groups or ideologies, through computer network attacks or cyber exploitation. The latter, by contrast, concerns the use of the internet, social media platforms and MSM by terrorist actors, particularly as a means of radicalisation through cyber-propaganda (Cortez, 2021)

[64] For a more detailed examination of this subject, see the report published by the Institute for Economics & Peace "Lone Wolf and Youth Terrorism" (Institute for Economics & Peace, 2025a).

Appendix B.2 – The Jihadist Radicalisation Model

The jihadist radicalisation process is often represented through a staged framework developed by prominent scholars such as Wictorowicz (2005), Silber & Bhatt (2007) and Sagean (2008), (cited by Cortez, 2021). Although each author offers nuances, their models converge around a four-phase structure:

1. Cognitive Opening / Pre-Radicalisation: Triggered by crises or perceived injustice, this phase marks a growing receptiveness to radical worldviews;
2. Religious Seeking / Self-Identification: he individual reinterprets their identity through a radical Islamist lens, often adopting a binary "us vs. them" worldview;
3. Identity Alignment / Indoctrination: Indoctrination intensifies through ideological reinforcement within closed communities or online ecosystems. Violence is gradually justified as a sacred duty;
4. Socialisation / Jihadisation: Full integration into jihadist networks occurs, often culminating in operational planning or support for terrorist actions.

An important dynamic in jihadist radicalisation, as highlighted by Cortez (2021), is the crime-terror nexus: the strategic recruitment of individuals with criminal pasts. These individuals provide tactical advantages such as: i) Access to illicit firearms and materials; ii) Experience with clandestine behaviour, reducing the risk of early detection; iii) Psychological desensitisation to violence, easing the adoption of terrorist methods. This nexus reflects a deliberate operational logic, in which terrorist groups prioritise practicality over ideological purity during recruitment.

Appendix B.3 – Strategic Logic and Operational Areas of Radicalisation Prevention

The strategic rationale of terrorism prevention is grounded in the premise that anticipating threats is more effective and less disruptive than responding after violent acts occur. This logic is based on strategic foresight and proactive intervention, which demand political will, institutional coordination, and analytical capacity (Schmid, 2021; Olech, 2021).

Prevention implies “backward reasoning”, meaning identifying early warning signs through an understanding of past trends and future projections (Schmid, 2021). Intelligence analysis must thus be complemented by robust legal frameworks and coordinated actions that balance security with democratic liberties.

According to Olech (2021), strategic forecasting is not merely a matter of intelligence analysis, it is also a political task. A state's security is deeply intertwined with its political orientation and institutional capacity. Strategic intelligence agencies must carry out comprehensive risk assessments that not only identify likely attackers or targets, but also anticipate the broader impact of threats on social cohesion, institutional credibility, and national stability. However, in order to be effective, they need to depend on the existence of robust legal frameworks, a clear institutional mandate for pre-emptive action and political will to act, all while preserving democratic values and civil liberties.

Technological sophistication is also essential. Terrorist actors increasingly exploit digital environments, via online propaganda, encrypted messaging platforms, AI algorithms and visual manipulation techniques (e.g., deepfakes), to radicalise, recruit and mobilise individuals globally (Institute for Economics & Peace, 2025a). Consequently, modern prevention strategies must incorporate digital monitoring tools, behavioural analytics, and interdisciplinary teams capable of interpreting complex data ecologies.

Drawing on Cortez (2021), seven operational priorities are essential:

1. Understanding the phenomenon of violent radicalisation: A thorough and interdisciplinary grasp of radicalisation, incorporating insights from criminology, sociology, psychology and political science;
2. Countering propaganda, hate speech and disinformation: Public resilience must be reinforced through media literacy training, critical thinking and active civil society engagement, equipping individuals to resist manipulative content;[65]
3. Preventing radicalisation in prisons: As correctional environments are often exploited by extremist networks, targeted measures such as de-radicalisation programmes, inmate screening, and psychosocial interventions are crucial;
4. Promoting awareness and inclusive education: Citizenship education, grounded in respect for diversity, democratic values, and human rights, acts as a vital inoculation against early radicalisation;

[65] The collection of intelligence through Human Intelligence (HUMINT) plays a crucial role in the early detection of radicalisation networks and in monitoring extremist narratives disseminated within community settings. This contributes to a more effective and sustained response by both authorities and civil society actors. (Cortez, 2021g; TPCE, 2021)

5. Engaging young people: Youth engagement initiatives must empower younger generations as ambassadors of inclusion, offering them meaningful alternatives to extremist narratives and fostering a sense of belonging;
6. Strengthening the security dimension through multi-actor cooperation: Prevention cannot rely solely on law enforcement. It must be articulated across sectors, involving educational, social, health and community-based stakeholders in a coherent framework;[66]
7. Enhancing international cooperation: Given the cross-border nature of radicalisation and terrorism, interinstitutional coordination, transnational intelligence-sharing, and harmonisation of legal frameworks are vital for timely and effective intervention.

A preventive strategy must therefore be multidimensional, transdisciplinary, and future-oriented, integrating technological tools with societal engagement to mitigate the evolving threats posed by violent extremism.

Appendix B.4 – Operational Tools and Preventive Practices

The prevention of violent radicalisation requires a layered combination of clinical tools, community engagement, and institutional strategies. Two specialised instruments are particularly noteworthy: the TRAP-18 (Terrorist Radicalisation Assessment Protocol) and the HCR-20 v3 (Historical Clinical Risk Management), used by professionals to identify behavioural and contextual risk indicators (Nowopolski et al., 2018).

The TRAP-18, developed by Meloy (2021), focuses on lone actors unaffiliated with formal terrorist organisations by assessing indicators like fixation, identification, pathway behaviour and ideological framing. Meanwhile, the HCR-20 v3 combines historical, clinical and risk management factors, offering flexibility and broader applicability (Douglas *et al*., 2014). The latter examines historical factors (e.g., prior violence, substance misuse), clinical indicators (e.g., mental health status), and risk management elements (e.g., social support and monitoring capacity). Both tools, however, depend on sensitive data and qualified analysts, and face challenges in multicultural contexts. Complementary to clinical diagnostics, community-based strategies such as community policing and strengthened

[66] Within this dimension, reference is made to the set of tools, policies, and security interventions employed by States and competent authorities to prevent, detect, and neutralise radicalisation processes that may lead to violent extremism or terrorism. This includes, the surveillance and monitoring of individuals, information sharing at national and international levels, legal instruments applicable to this domain, and the training of police forces and intelligence services.

HUMINT collection (OSCE, 2014) help detect early signs of radicalisation. By fostering trust and proximity, law enforcement can work with educators, religious leaders, and local actors to gather informal, yet valuable intelligence.

Public awareness campaigns and deradicalisation programmes also play a crucial role. The UK's "Act Early" (Action Counters Terrorism, 2025) and Poland's "4U!" (University of Gdansk, 2024) exemplify efforts to engage civil society and build resilience through education and inclusion.

Institutional efforts, such as those of the TPCE in Poland, provide specialised training comprising five core modules: radicalisation awareness; behavioural protocols in terror scenarios; emergency first aid; cybersecurity; and strategic infrastructure protection. (TPCE, 2021; TPCE, 2025; Wysocka, 2023). At European level, the EU Strategic Agenda 2023–2027 prioritises reintegration, particularly of women and children returning from conflict zones, through multidisciplinary teams offering psychological, social, and vocational support (CDCT, 2023). They also address identity reconstruction, emotional rehabilitation, and social reinsertion through housing, employment, and educational support. Reintegration efforts, although complex and long-term, are essential to reducing recidivism and preventing renewed exposure to extremist environments.

In the digital sphere and at the European level, ECTC has developed specialised units[67] to detect and remove violent extremist content. Their action is strengthened by strategic partnerships with online service providers[68], while promoting more robust tools for OSINT and confidential intelligence analysis (Cortez, 2021). The production of intelligence, often composed of non-judicially admissible information, has become a cornerstone of proactive criminal investigation. This shift demands not only technological sophistication but also legal foresight, political will and a multidisciplinary approach capable of detecting, disrupting and neutralising threats before they materialise.

Effective prevention now depends on the integration of digital forensics, AI-driven analytics, and transnational cooperation to anticipate and neutralise threats. In summary, preventive practices must blend scientific, social, and strategic elements. Their success

[67] IRU – Internet Referral Unit

[68] The IRU operates in close cooperation with social media platforms (such as Meta/Facebook, TikTok, Telegram or Tinder) and search engines (including Google and Opera), with the aim of detecting, analysing, and referring terrorist content for removal. This collaborative effort seeks to ensure that digital environments are not exploited for radicalisation, recruitment, or operational planning, while also preserving fundamental rights such as freedom of expression and privacy. (EUROPOL, 2025)

hinges on international cooperation, political will, legal foresight, and societal engagement across multiple sectors.

Appendix B.5 – Profiles, Typologies and Operational Patterns in Lone Wolf Terrorism

Lone Wolf terrorism is characterised by individuals who carry out violent acts independently, without any structural affiliation to terrorist organisations. However, this operational autonomy does not imply ideological isolation, as many of these actors are influenced by broader extremist narratives disseminated online, particularly by groups such as ISIS or Al-Qaeda (Wysocka, 2023; Silva, 2020).

Academic literature identifies three main subtypes of Lone Wolf terrorists, as proposed by Duarte (2013), where each is defined by the degree of isolation and support involved:

- Completely isolated individuals: These actors plan and execute attacks alone, without any external assistance, whether logistical, ideological, or material. Their radicalisation process is usually self-directed and their actions often reflect personal grievances or extremist convictions formed in isolation;
- Individuals with facilitators: The actor maintains contact with one or more facilitators, either online or in person. These facilitators may offer ideological support (e.g., via extremist forums or social media) or limited logistical aid (such as advice, resources, or encouragement), without constituting a formal terrorist cell. The boundaries between inspiration and incitement are often blurred in these cases;
- Informal autonomous groups: This category includes small groups, often composed of relatives or acquaintances, that operate without a hierarchical structure or formal linkage to terrorist organisations. Although collectively active, they retain a Lone Wolf dynamic by functioning outside institutional command chains and forming spontaneously based on shared radical beliefs.

These distinctions suggest that autonomy exists along a continuum and may evolve throughout the radicalisation process (Pantucci, 2011). Motivations vary widely and typically combine ideological convictions with emotional distress, psychological disturbances, personal grievances or a desire for notoriety (Bakker & Graaf, 2010; Spaaij, 2012; Yitzhak, 2013). The absence of a uniform sociological or psychological profile complicates early detection and renders many conventional risk modelling tools ineffective.

Consequently, Lone Wolves are often described as "black swans" [69], rare but highly disruptive actors whose emergence defies accurate prediction.

Operationally, these individuals rely heavily on OSINT content to plan their attacks, including tutorials, ideological material and technical guidance accessible through MSM, encrypted digital platforms and social media. This digital dependence, coupled with the absence of contact with known networks, severely limits the effectiveness of traditional surveillance mechanisms (Institute for Economics & Peace, 2025). Their unpredictability is further exacerbated by emotional volatility, moments of personal crisis and sudden behavioural changes.

In this sense, Lone Wolf terrorism demands a paradigm shift in counter-terrorism: from a model focused on intercepting coordinated plots to one capable of identifying diffuse, solitary and ideologically motivated actors through interdisciplinary cooperation, digital monitoring and robust early-warning mechanisms integrated into social institutions (Bakker & Graaf, 2010).

Notable examples include Anders Breivik (Norway in 2011), whose anti-immigration and anti-Islamic ideology led to the murder of 77 people (Breivik, 2011; BBC, 2011); Omar Mateen (USA in 2016), influenced by jihadist online content and identity-related conflict; and Mohamed Merah (France in 2012), who, despite previous jihadist contacts, acted alone during his attacks. These cases illustrate the tactical and psychological diversity inherent in the Lone Wolf model.

Preventive efforts require robust assessment tools such as TRAP-18 and HCR-20 v3, which offer structured frameworks to identify behavioural and psychopathological risk indicators (Meloy, 2021; Douglas *et al*., 2014). However, the effectiveness of these instruments depends on interdisciplinary expertise and access to sensitive data. Community-based approaches, grounded in HUMINT and OSINT and proximity policing, remain essential for early intervention by fostering trust and enabling the informal identification of behavioural anomalies (OSCE, 2014; TPCE, 2021).

Nonetheless, ethical challenges persist, particularly concerning potential mass surveillance, the stigmatisation of Muslim communities, and the erosion of civil liberties. Effective prevention strategies must therefore strike a careful balance between safeguarding public security and upholding democratic rights. Psychosocial, educational and

[69] These attacks are rare and unpredictable, but often have a significant impact. For a more detailed analysis of the "black swan" theory, see Appendix C – "Black Swans" Theory.

communicational approaches should be integrated to promote resilience and critical engagement with extremist content online (Duarte, 2013; Institute for Economics & Peace, 2025a).

Appendix B.6 – Strategic Foundations and Ideological Links in Freelance Terrorism

Freelance Terrorism reflects the strategic decentralisation of global jihadism, emerging during the third phase[70] of its evolution, characterised by the encouragement of autonomous attacks by ideologically aligned individuals. Unlike traditional models based on hierarchical structures, this typology is defined by operational autonomy combined with varying degrees of ideological or logistical dependence on groups such as Al-Qaeda and Daesh (Duarte, 2013; Silva, 2020).

This shift is largely a response to intensified counter-terrorism measures, which have made coordinated operations increasingly difficult. Jihadist organisations have consequently prioritised incitement through online propaganda, sermons and encrypted communications, facilitating individual radicalisation in Western societies (Reinares & García-Calvo, 2013). Although often labelled as "home-grown" or "individual jihadists", these actors are united by the duality of acting independently while maintaining ideological affinity with transnational movements (Yitzhak, 2013; Duarte, 2013).

In terms of operational typology, Silva (2020) identifies three subtypes: i) individuals radicalised online and incited through propaganda, without direct organisational contact; ii) those who receive limited logistical or technical support, such as basic training or access to weapons; iii) and small, informally structured cells aligned with jihadist goals. Many experience social marginalisation, frustration, or cultural exclusion, which fosters identity-based affiliation to jihadist causes (Reinares & García-Calvo, 2013; Silva, 2020; Wysocka, 2023). These actors are frequently young men (18-45), often second-generation immigrants, marked by social exclusion, identity crises or unresolved psychological conflict (Yitzhak, 2013; Wysocka, 2023). Most attacks occur near the perpetrator's residence (typically within 2 to 10 km), reinforcing a localised operational logic (Silva, 2020).

Operationally, freelance attacks typically involve accessible methods, such as knives, vehicles or improvised explosives, promoted through jihadist propaganda for their simplicity

[70] First phase: structured networks and centralised operations (under Al-Qaeda leadership) during 1990s and early 2000s; Second phase: broader transnational expansion, emerging regional affiliates and more diffuse modes of action; Third phase: strategic decentralisation, where jihadist organisations encourage individual actors to execute attacks in their home countries, with minimal support (Duarte, 2013; Reinares & García-Calvo, 2013).

and psychological impact. Targets tend to be symbolically or socially significant and many perpetrators share manifestos or declarations prior to the attack, reinforcing ideological motivations and potentially triggering copycat phenomena (EUROPOL, 2014–2024; Spaaij, 2012). Perpetrators typically plan operations using OSINT tools and local knowledge, enabling them to exploit vulnerabilities on densely populated or emblematic sites, with minimal risk of detection (Spaaij, 2012; Wysocka, 2023). Cases such as the Berlin truck attack (2016) and the Woolwich murder (2013) illustrate the hybrid nature of Freelance Terrorism, where local grievances converge with global jihadist narratives to produce highly lethal outcomes.

Preventing freelance terrorism requires a paradigm shift from organisational surveillance to early detection of individual radicalisation. This includes behavioural tools such as TRAP-18 and HCR-20 v3 (Meloy, 2021; Douglas *et al*., 2014), complemented by technological approaches like biometric analysis, geoprofiling[71], and behavioural monitoring. Yet, ethical concerns remain salient, particularly regarding mass surveillance and the stigmatisation of Muslim communities (Reinares & García-Calvo, 2013). In this regard, community-based strategies and psychosocial prevention, supported by local actors (e.g. educators, psychologists and religious leaders) and HUMINT, offer more sustainable alternatives (TPCE, 2021; ICCT, 2025). Building trust within vulnerable communities is essential to detect early signs of radicalisation without eroding civil liberties. Moreover, emerging digital threats, including algorithmic radicalisation and deepfakes, demand updated regulation, advanced technical capacities, and intensified international cooperation (Cortez, 2021g).

Freelance Terrorism, as a doctrinal and operational innovation, bridges global ideological warfare with locally executed acts of violence. Understanding and addressing this phenomenon requires a multidisciplinary and ethically informed strategy that integrates global security dynamics with local resilience mechanisms.

[71] Geoprofiling (or geographic profiling) is a spatial analysis technique used in criminal investigations to estimate the most likely location of an offender´s residence, workplace, or other points of interest, based on the geographical distribution of previous offences. This method is based on the assumption thar offenders tend to commit crimes within their so-called “comfort zones” (e.g., residential neighbourhoods or familiar areas), while avoiding locations too close to home to minimise suspicion and too far away due to increased effort and risk. Initially developed for identifying serial killers and sexual offenders, geoprofiling can also be adapted to the context of freelance terrorism in order to anticipate target selection or movement patterns of the attacker (Rossmo, 2000; Silva, 2020)

APPENDIX C - "BLACK SWANS" THEORY

When reflecting on the nature of Islamic terrorism, particularly the individual form addressed in this dissertation, it is difficult not to associate it with the “Black Swan” theory developed by Professor Nassim Nicholas Taleb. This theory invites a careful and profound reflection on how the terrorist threat has been perceived. According to Taleb, for an event to be considered a “Black Swan”, it must fulfil three criteria (Taleb, 2020, cited in Wysocka, 2023, pp. 45-46): i) It must be an atypical phenomenon, something that lies outside the realm of regular expectations, in that no past occurrence convincingly points to its possibility; ii) It must have an extreme impact on reality; iii) Although the event is atypical, human nature leads us to seek explanations or narratives to make it seem predictable after the fact.

These three characteristics clearly demonstrate that individual terrorists are, in fact, “Black Swans”. Their actions remain atypical (even though they have become more visible in Europe in recent years), difficult to anticipate, and, to some extent, incomprehensible. It is also important to highlight that, according to this theory, “Black Swans” do not fit into established models, as they remain beyond the boundaries of observed and analysed reality (Taleb, 2020, cited in Wysocka, 2023, pp. 45-46). Even when their existence is acknowledged after an attack, efforts are focused on preventing future occurrences and analysing similar Black Swans, a challenge in itself, as potential future manifestations cannot yet be recognised (Taleb, 2020, cited in Wysocka, 2023, pp. 45-46).

This phenomenon is referred to as “Black Swan blindness”, which can manifest in two forms (Taleb, 2020, cited in Wysocka, 2023, pp. 45-46): i) When Black Swans are integrated into political discourse and appear in MSM narratives; ii) When Black Swans are not addressed at all, because they are excluded from existing models.

Based on this analysis, a specific terminology can be adopted in relation to individual terrorism, whereby its existence is understood to fall within the second scenario described above. Broadly speaking, it may be argued that these actors are the “blackest” of Black Swans, as until recently, they were not granted substantial recognition and were not seen as a tangible threat to international security (Wysocka, 2023, pp. 45-46). It should also be emphasised that, to date, no coordinated international response has been developed specifically to address the phenomenon of individual terrorism.

APPENDIX D – COUNTER-TERRORISM FRAMEWORKS IN PORTUGAL, POLAND AND FRANCE

Appendix D.1 – Counter-Terrorism Framework in Portugal

Portugal's counter-terrorism framework is structured around a centralised and hierarchical model, ensuring close coordination across strategic, operational and judicial levels. Intelligence operations are led by SIRP, with preventive and investigative actions distributed among internal security forces and specialised judicial authorities. An essential component of the national security apparatus is the terrorist threat assessment system, managed exclusively by SIS, based on a five-level scale where Level 1 represents extreme threat and Level 5 denotes negligible threat (SIS, 2024). UCAT[72] serves as a key advisory body to the political and strategic leadership, supporting the national decision-making process through integrated assessments, regular situational reports and systematic intelligence sharing across national agencies. It also ensures strategic inter-agency coordination and oversees the implementation of the ENCT, operating as the principal forum for threat assessment and intelligence sharing.

At the operational level, both the GNR and the PSP deploy specialised tactical units, while the PJ leads criminal investigations through its counter-terrorism, financial intelligence units. The GNR also operates with units focused on fiscal actions (*Unidade de Ação Fiscal* – UAF) combating financing of terrorism in a supportive role with PJ and with its Boarder and Coast Control Unit (*Unidade de Controlo, Costeiro e Fronteiras* – **UCCF**)[73]. Judicial oversight is entrusted to the DCIAP[74], responsible for supervising complex investigations and authorising special investigative measures such as surveillance, communication interception and infiltration operations.

The following table provides a summarised overview of the main entities, their supervising ministries, and their core counter-terrorism competencies.

---

[72] See Preamble and Art.º 2.º of Regulatory Decree n.º 2/2016 (Decreto Regulamentar n.º 2/2016, de 23 de agosto)

[73] The UCCF is responsible for the management and operation of SIVICC (*Sistema Integrado de Vigilância, Comando e Controlo*), a surveillance and command system designed to detect and combat threats across multiple domains along the Portuguese boarders, including terrorism, as established by Joint Ministerial Dispatch n.º 386/200 (Despacho Conjunto n.º 386/2006, de 9 de maio, 2006).

[74] In the counter-terrorism context, the DCIAP plays a critical role in the judicial validation of special investigative measures such as surveillance, communications interception, infiltration operations and undercover activities, because it is entrusted with leading the prosecution in particularly complex proceeding – Art.º 2.º of LOIC; MP (2025).

Table 1 - Institutional Framework of Counter-Terrorism in Portugal: Entities, Competencies and Legal Mandates

Entity	Type	Main Competences	Legal Framework / Source
SIRP	Intelligence	Coordination of intelligence services; political decision support; threat anticipation	Lei n.º 9/2007, de 19 de fevereiro; (SIRP, 2025)
SIS	Intelligence	Internal security intelligence; HUMINT and OSINT focused on terrorism and extremism	Lei n.º 9/2007, de 19 de fevereiro; (SIS, 2024)
SIED	Intelligence	Foreign intelligence; external threats to national defence	Lei n.º 9/2007, de 19 de fevereiro; (SIED, 2025)
CISMIL	Intelligence	Military intelligence; support for international missions and defence operations	(EMGFA, 2025)
GNR - GIOE, UAF and UCCF	Law Enforcement	Tactical interventions (GIOE); fiscal action unit (UAF); border security (UCCF)	LOGNR - Lei n.º 63/2007, de 6 de novembro; (GNR, 2025)
PSP - GOE	Law Enforcement	Urban policing; high-risk tactical interventions (GOE)	LOPSP - Lei n.º 53/2007, de 31 de agosto; (PSP, 2025)
PJ - UNCT and UIF	Law Enforcement	Criminal investigations; counter-terrorism networks; terrorism financing and cyberterrorism	LOPJ - Decreto-Lei n.º 275-A/2000, de 9 de setembro; (PJ, 2025)
UCAT	Strategic Coordination	Inter-agency coordination; implementation of national counter-terrorism strategy; threat assessments	Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio
DCIAP	Judicial Authority	Judicial oversight; direction of terrorism investigations; validation of special investigative measures	Art.º 2.º da LOIC; (DCIAP, 2025)

The legislative framework underpinning these institutional structures is robust. Early legislative sensitivity to terrorism dates back to the creation of SIRP in 1984, following terrorist incidents involving foreign embassies in Lisbon[75]. The LSI sets the strategic foundations, defining internal security as the state-led activity to ensure public order, protect individuals and property and uphold the democratic rule of law[76]. The cornerstone of counter-terrorism legislation remains the Lei n.º 52/2003, de 22 de agosto (2003), enacted to comply with Council Framework Decision 2002/475/JHA and subsequently adapted to incorporate Directive (EU) 2017/541[77]. The law criminalises terrorist organisations, preparatory acts, terrorist financing and activities such as recruitment, training, and travel for terrorist purposes, with strict sentencing regimes. Penalties range from 8 to 20 years depending on the severity of the crime and the degree of involvement.

[75] In 1984, following terrorist attacks that occurred on Portuguese soil, notably the attack on the Israeli embassy in 1979 and the assassination of the commercial attaché of the Turkish embassy.
[76] See Art.º 1.º n.º 1 and 3 of Lei n.º 53/2008, de 29 de agosto; the concept of internal security refers to the set of state-led activities aimed at ensuring public order, safety, and tranquillity, protecting individuals and property, preventing and repressing crime, and upholding the normal functioning of democratic institutions and the rule of law.
[77] This law was enacted in compliance with Council Framework Decision 2002/475/JHA and subsequently amended to accommodate Directive (EU) 2017/541 of the European Parliament and the Council, of 15 March.

Appendix D.2 – Counter-Terrorism Framework in Poland

Poland's counter-terrorism framework is built upon a dual structure of strategic intelligence agencies and operational law enforcement and military units. Intelligence functions are primarily executed by four core agencies: ABW, responsible for internal threats and prevention of terrorism; AW, focused on external terrorist threats; SWW, dealing with external military threats; SKW, securing internal military environments. These agencies report both to their ministries and to the Minister Coordinator for Special Services.

Operational and tactical counter-terrorism actions are entrusted to specialised police and military units. The PP[78] deploys tactical units like SPAP and BOA[79]. The SG focuses on border security and prevention operations. The ŻW and the WS, with elite units such as the GROM and FORMOZA, ensure military support to counter-terrorism efforts.

This integrated model reflects Poland's proactive stance in anticipating and countering terrorist threats, even within a context of low immediate risk. For a detailed systematisation of the main counter-terrorism entities, their competencies, and legal frameworks, see Table 2 below.

Table 2 - Institutional Framework of Counter-Terrorism in Poland: Entities, Competencies and Legal Mandates

Entity	Type	Main Competences	Legal Framework / Source
ABW	Intelligence	Internal security, terrorism prevention, judicial police powers	Ustawa z dnia 24 maja 2002 r.; (ABW, 2025)
AW	Intelligence	Foreign intelligence, international terrorism analysis	Ustawa z dnia 24 maja 2002 r.; (AW, 2025)
SWW	Intelligence	External military intelligence, terrorism in conflict zones	(SWW, 2025)
SKW	Intelligence	Internal military security, counter-terrorism in the Armed Forces	(SKW, 2025)
Minister Coordinator for Special Services	Coordination	Oversight and coordination of intelligence agencies	(Chancellery of the Prime Minister, 2025)
PP – SPAP and BOA	Law Enforcement	Tactical interventions, Anti-Terrorist operations	Act of 6 April 1990 on the Police; (Zubrzycki, 2017; PP, 2025)
SG	Law Enforcement	Border security, reconnaissance, threat detection	Ustawa o Straży Granicznej; (Puacz-Olszewska, 2019)

[78] According to the Art.º 17.º n.º 6 of the ACT of 6 April 1990 on the Police (1990) the Polish Police are authorised to use lethal force against individuals reasonably suspected of planning or carrying out a terrorist attack.

[79] It operates as an elite tactical unit in high-risk and crisis situations, and also functions as a criminal police unit, responsible for reconnaissance, evidence gathering, intelligence collection, investigations, and the arrest of individuals associated with terrorist activities at a national level (Zubrzycki, 2017)

ŻW	Military Support	Military police, support to counter-terrorism	Ustawa o Żandarmerii Wojskowej; (EUROGENDFOR, 2025)
WS – GROM and FORMOZA	Military Special Forces	Land, maritime, and underwater counter-terrorism operations	(MND, 2025; MND, 2023; Zubrzycki, 2015)

Poland thus has a diverse set of specialised intelligence agencies operating at the strategic level in the fight against terrorism. These entities play a central and pivotal role in decision-making, the implementation of measures, and in ensuring state security, primarily through the gathering of intelligence on terrorist threats (Olech, 2021). The main missions of these agencies include maintaining an appropriate security level in response to threats, protecting national interests, and combating threats originating both externally and internally, particularly in the context of counter-terrorism (Olech, 2021).

Poland's legislative framework for counter-terrorism is distinguished by its emphasis on pre-emptive intervention and rapid operational capabilities. The central piece of legislation is the Anti-Terrorism Act 2016, which systematically redefined the powers attributed to security and intelligence services in the prevention and suppression of terrorist threats. One of the Act's most significant innovations lies in enabling the SFS to undertake real-time surveillance operations without prior judicial oversight, including electronic communication interceptions and immediate access to personal and financial data. Such provisions are justified by the necessity to counter stealthy, decentralised threats, particularly those associated with Freelance Terrorism.

Although Poland lacks a unified and updated national counter-terrorism plan, it has developed a series of preventive and educational initiatives aimed at mitigating the effects of terrorist threats and strengthening civil society's resilience.

One of the most significant tools is the Terrorism Prevention Guide, published by the TPCE. This manual provides civilians with essential guidelines on how to act in emergency situations, promoting practical advice for minimising casualties and improving individual and collective preparedness during terrorist incidents (TPCE, 2021). The guide includes instructions on evacuation procedures, first aid techniques, situational awareness, and strategies to maintain calm and assist security forces during crises. Complementing this, the "4U!" campaign provides multimedia resources on how to react to various types of attacks, including shootings and chemical or biological incidents. These efforts aim to enhance public resilience, acknowledging that a vigilant and trained civilian population is a crucial layer in counter-terrorism strategies.

These initiatives are rooted in the assumption that a vigilant and well-informed society is a critical component of counter-terrorism strategies. By raising public awareness and preparedness, Poland seeks not only to limit the potential impact of attacks but also to reinforce the legitimacy and effectiveness of the broader security apparatus. This dual approach, strong legislative measures combined with public education and training, illustrates Poland's strategy of reinforcing societal resilience and operational efficiency, mitigating the absence of a centralised strategic document.

Appendix D.3 – Counter-Terrorism Framework in France

France's counter-terrorism framework integrates intelligence, law enforcement and judicial entities under a hierarchical and coordinated structure. External and defence-related intelligence are the responsibility of the DGSE, DRSD and DRM under the MND, while internal security is ensured by the DGSI under the MIA. Economic and financial intelligence is handled by DNRED and TRACFIN (under the ME) and terrorism prosecutions are centralised in the PNAT[80] (MJ).

At the operational and tactical level, several specialised units operate under the MIA, notably the RAID, BRI[81], CRS of PN, and the GIGN under the GN. These forces are complemented by local-level cooperation with the *Police Municipale*, whose role in first response has been increasingly professionalised and integrated into the national counter-terrorism framework (Olech, 2022a; Touati, 2023).

Coordination of intelligence sharing and threat assessments is centralised in the DGSI, following the transfer of responsibilities from UCLAT in 2019. DGSI, is thus, now responsible for organising regular meetings to assess threats, conducting cross-cutting analyses, sharing intelligence and issuing alerts and reports, serving as the central hub for information gathering by various services in the fight against terrorism, coordinating investigations, managing the national counter-terrorism alert system (*Plan Vigipirate*) and producing threat assessment reports and profiles (PoliceFR, 2025). For a systematised overview of France's counter-terrorism entities, competencies and legal mandates, see Table 3 below.

[80] It has jurisdiction to prosecute, adjudicate, and sentence in two primary areas: i) offences related to terrorism; ii) offences concerning the proliferation of weapons of mass destruction

[81] Combines tactical intervention capabilities in high-risk crisis situations with judicial police functions, particularly through its specialized units known as BRI de la Police Judiciaire.

Table 3 - Institutional Framework of Counter-Terrorism in France: Entities, Competencies and Legal Mandates

Entity	Type	Main Competences	Legal Framework / Source
DGSE	Intelligence	External intelligence, counter-terrorism, cybersecurity	(MND, 2025)
DRSD	Intelligence	Threat and risk analysis in defence environments	(MND, 2025a)
DRM	Intelligence	Military intelligence for operational deployment	(MND, 2025b)
DGSI	Intelligence	Internal security, counter-terrorism, counter-espionage	(MIA, 2025)
DNRED	Intelligence	Border control intelligence, organised crime prevention	(ME, 2025a)
TRACFIN	Intelligence	Fight against terrorist financing	(ME, 2025b)
PNAT	Judicial Authority	Centralised prosecution of terrorism and weapons of mass destruction crimes	(MJ, 2019)
PN – BRI, RAID, CRS	Law Enforcement	Tactical intervention, judicial police functions	(PN, 2025a; 2025b; 2025c)
GN – GIGN	Law Enforcement	High-risk counter-terrorism operations (land, air, maritime)	(MIA, 2025b; Olech, 2021)
DGSI – SDAT, SAT	Law Enforcement	Investigation and prevention of terrorist activities	(MIA, 2024; 2025c)
Police Municipale	Local Law Enforcement	Local preventive action and armed response support	(Olech, 2022a; Touati, 2023)

A distinguishing feature of the French system is the integration of preventive strategies against radicalisation, combining educational, digital and community-based initiatives, alongside expanded digital surveillance policies (Olech, 2022a; Touati, 2023) although these policies are often contested on human rights grounds. The French framework, thus, combines a sophisticated, hierarchical structure with preventive strategies and robust operational capabilities, often serving as a benchmark within the European context.

France's counter-terrorism legal framework has evolved from emergency measures to a consolidated system of preventive and repressive instruments. A major turning point was the adoption of *loi SILT*, which integrated into ordinary law powers from the post-2015 state of emergency, such as administrative searches without judicial warrants, house arrests, closure of radical places of worship, and movement restrictions. The *loi SILT* also introduced algorithmic surveillance tools, known as "black boxes" (Faustino, 2018; Olech, 2022a)[82].

Complementing these measures, Law n.º 2016-987 of 21 july 2016, created administrative controls for individuals convicted of terrorism-related crimes, extending surveillance[83] after their release. Border control was also reinforced by prolonging identity checks in border zones to twelve hours to prevent the entry of FTFs (Gouvernement Français, 2006; Faustino, 2018; Olech, 2022a).

[82] These algorithmic tools enable French Intelligence services to flag suspicious activity online without prior judicial authorization, raising ongoing concerns about the proportionality of such intrusions in cyberspace. (Olech, 2021)

[83] These measures have a maximum duration of twelve months and include obligations such as travel restrictions or electronic surveillance (Olech, 2022a).

France's counter-terrorism operational capacity is significantly reinforced by the *Plan Vigipirate* and *Operation Sentinelle*, two complementary initiatives that form the backbone of its national security strategy. The *Plan Vigipirate* is a permanent national alert and security framework designed to prevent and mitigate terrorist threats, that consists of over 300 preventive measures across thematic areas such as transportation security, cybersecurity, crisis management and public awareness. Its implementation relies not only on state authorities but also on local entities, private sector organisations and citizens, promoting a whole-of-society approach to resilience. Public participation is fostered through educational initiatives like the "assume, alert, protect" campaign[84], aimed at improving individual preparedness during attacks (SGDSN, 2016; Olech, 2022a).

In parallel, *Operation Sentinelle* consists on military personnel patrolling sensitive areas such as transportation hubs, religious sites, tourist attractions and major public gatherings (Troin & Léonard, 2016; SGDSN, 2016). It significantly expanded the visible military presence compared to the *Plan Vigipirate* earlier deployments, contributing to deterrence through visibility and rapid response capabilities. Although soldiers involved in *Operation Sentinelle* are authorised to carry arms and use lethal force to prevent imminent threats, their legal powers are limited to defensive actions; they are not empowered to perform criminal investigations, carry out judicial arrests[85], or conduct identity checks, tasks which remain the responsibility of law enforcement (Troin & Léonard, 2016; SGDSN, 2016; Olech, 2022a).

The combination of *Plan Vigipirate* and *Operation Sentinelle* illustrates France's strategic approach to counter-terrorism: integrating military and police resources within a coordinated framework to enhance national preparedness and public security. While praised for its effectiveness in countering threats, this model has also raised discussions about the balance between heightened security measures and the protection of civil liberties in a democratic context.

[84] This triad is part of the public behavioural guidance disseminated under the *Plan Vigipirate* framework. It promotes three simple reflexes for civilians in the event of a terrorist attack: i) Assume responsibility by identifying and avoiding danger zones; ii) Alert the emergency services by providing concise and accurate information; iii) Protect oneself by seeking shelter, avoiding exposure and waiting for rescue. This strategy seeks to empower citizens as proactive actors in national security, while simultaneously reinforcing situational awareness and resilience across society. (SGDSN, 2016)

[85] They may proceed with an arrest, but must be immediately handed over to the competent law enforcement authorities. (Troin & Léonard, 2016; SGDSN, 2016)

Appendix D.4 – Comparative Overview of the Countries

Table 4 - Comparative Overview of National Counter-Terrorism Entities

Dimension	Portugal	Poland	France
Domestic Intelligence Agency	SIS – no criminal investigative powers	ABW – with police powers	DGSI – with judicial police powers
Foreign Intelligence Agency	SIED	AW	DGSE
Military Intelligence	CISMIL (under EMGFA, outside of SIRP)	SWW e SKW (under MND and Coordinator of Special Service)	DRSD e DRM (under MND)
Judicial Police Autonomy	PJ – autonomous with UNCT	BOA of the Police and ABW	Functions distributed across DGSI, PN and GN
Prosecutorial Body for Terrorism	DCIAP (broad competence, but not exclusively for terrorism)	Regional prosecutors in coordination with ABW	PNAT – exclusive national body
Operational Coordination Unit	UCA under SSI	No formal unit; ABW acts as coordinating entity	DGSI (since 2019, after the disbanding of UCLAT)
Tactical Counter-Terror Units	GOE-PSP e GIOE-GNR (dual model)	BOA, SPAP, GROM, FORMOZA	RAID, BRI, GIGN
Civil-Military Integration	Cooperation in emergencies and international missions	Strong involvement of the AF and ŻW	Institutional integration of civil and military forces (e.g., Operation Sentinelle)
Civic Preparedness Programmes	No national programme; sector-specific resilience plans	TPCE – unique in Europe	Local educational campaigns; no centralised national programme
Financial Intelligence Unit	Embedded within the PJ with support from the UAF (GNR)	Embedded within the ABW	TRACFIN – structurally independent financial intelligence unit

Table 5 - Comparative Legislative Frameworks

Dimension	Portugal	Poland	France
Core Anti-Terrorism Law	Law no. 52/2003 – defines terrorism and criminalises associated behaviours	2016 Anti-Terrorism Act – wide-ranging	Law no. 2017-1510 (SILT); codifies emergency powers
Preventive Detention Powers	Limited; only with judicial order and strong grounds (CPP Art.º 187)	Up to 30 days without formal charge (controversial)	Permits administrative restrictions, house arrest, etc.
Surveillance Measures	Requires judicial authorisation; concerns on lack of preventive powers	Extensive powers including communication interception, data access	"Black box" algorithmic surveillance authorised
Judicial Oversight	Judicial validation mandatory for searches, surveillance, etc.	Limited; judicial approval often not required before actions	Administrative control often replaces judicial approval
Definition of Terrorism	Indirectly defined via Art.º 2 of Law 52/2003	No general definition; uses operational categories	Defined in Penal Code, Titles II & III
Terrorist Financing	Criminalised (Art.º 5 Law 52/2003); "Strong" penalties (8–15 years)	Integrated into ABW functions; no separate agency	Criminalised; monitored by TRACFIN (financial intelligence)
Special Prosecutorial Body	DCIAP – broad jurisdiction, not terrorism-exclusive	Handled by regional prosecutors with ABW support	PNAT – specialised and exclusive terrorism prosecution unit
Cybersecurity & Digital Surveillance	General data protection applies; calls for reform	Permits data monitoring without consent; blacklists, AI use	Strong legal basis for digital surveillance and online policing

Border Control & FTFs	Aligned with EU acquis; no additional anti-FTF powers	Expanded powers including deportation, exclusion of foreigners	12-hour checks at borders; monitoring of returnees
Civil Liberties Concerns	Concerns over limited preventive tools & delays in approval	Criticised for overreach and weak safeguards	Praised for deterrence; criticised for erosion of liberties
Strategic Doctrine	ENCT – Resolution 7-A/2015; focus on coordination and resilience	No current national strategy; emphasis on TPCE and ABW coordination	*Livre Blanc* – doctrine of vigilance, resilience, pre-emption

In an increasingly interconnected and volatile global security landscape, international and European cooperation has become a fundamental pillar of national counter-terrorism strategies. Portugal, Poland and France are active participants in a range of platforms designed to enhance intelligence exchange, joint operations and coordinated responses to terrorist threats.

At the European level, Europol plays a pivotal role, particularly through its ECTC, which supports states members in information sharing, operational coordination, and strategic analysis (EUROPOL, 2025b). National Single Points of Contact (SPOC's) ensure 24/7 secure channels for international cooperation on terrorism cases (EUROPOL, 2025b). Interpol complements these efforts by facilitating global police cooperation. Its Counter-Terrorism Fusion Centre works to detect, prevent and disrupt terrorist activity worldwide, including through cooperation with EU states and UN mechanisms (INTERPOL, 2025).

Operationally, Portugal, Poland and France are also part of the ATLAS Network[86], a European platform that connects elite tactical police units from EU Member States. Created to improve the response to terrorism and high-risk threats, ATLAS Network enables joint training, scenario simulations and rapid deployment coordination (Lippay, 2021). Participating units include Portugal's GOE (PSP) and GIOE (GNR), Poland's BOA (and ŻW sometimes) and France's RAID and GIGN (Lippay, 2021)

On a global scale, the three countries align with the initiatives of the United Nations Office of Counter-Terrorism (UNOCT) and its Counter-Terrorism Centre (UNCCT). The UNOCT provides a common framework focused on preventing violent extremism, protecting human rights and reinforcing state capacity (UNOCT, 2024). Notably, Poland's TPCE was developed partly in alignment with UNCCT models and goals (UNOCT, 2024; UN, 2025).

[86] The ATLAS network of police tactical units has a Support Office at Europol, meaning that the ECTC coordinates cross-border operations by units from the Schengen Area countries and the United Kingdom. In order to share knowledge, individual ATLAS units join together in working groups on issues such as critical infrastructure, urban operational tactics, snipers, covert tactical action, negotiating skills, medical support and transport. (European Parliament, 2021)

APPENDIX E – STATISTICAL OVERVIEW OF TERRORIST ACTIVITY AND COUNTER-TERRORISM RESPONSES IN PORTUGAL, POLAND AND FRANCE (2013–2024)

Table 6 - Total number of arrests by affiliation

Year	Country	Jihadism	Left-Wing	Right-Wing	Separatism	Not Specified	Total
2013	Portugal	0	0	0	0	0	0
	Poland	0	0	0	0	0	0
	France	143	1	3	77	1	225
2014	Portugal	0	0	0	0	0	0
	Poland	0	0	14	0	0	14
	France	188	1	5	41	3	238
2015	Portugal	0	0	0	2	0	2
	Poland	4	0	13	0	0	17
	France	377	1	2	44	0	424
2016	Portugal	1	0	0	0	0	1
	Poland	5	0	1	0	0	6
	France	429	1	0	26	0	456
2017	Portugal	1	0	0	0	0	1
	Poland	2	0	0	0	1	3
	France	373	10	15	13	0	411
2018	Portugal	0	0	0	0	0	0
	Poland	0	0	0	0	2	2
	France	273	3	32	2	0	310
2019	Portugal	1	0	0	0	0	1
	Poland	2	0	2	0	0	4
	France	202	0	7	13	2	224
2020	Portugal	0	1	0	0	0	1
	Poland	8	0	1	0	0	9
	France	99	11	5	12	0	127
2021	Portugal	2	0	0	0	0	2
	Poland	0	0	0	0	3	3
	France	96	3	29	12	0	140
2022	Portugal	1	0	0	0	0	1
	Poland	0	0	0	0	0	0
	France	93	0	16	0	0	109
2023	Portugal	0	0	0	0	0	0
	Poland	1	0	0	0	0	1
	France	62	0	4	11	1	78
Total		**2363**	**32**	**149**	**253**	**13**	**2810**
Total Portugal		**6**	**1**	**0**	**2**	**0**	**9**
Total Poland		**22**	**0**	**31**	**0**	**6**	**59**
Total France		**2335**	**31**	**118**	**251**	**7**	**2742**

Source: Own elaboration based on TE-SAT reports (2014–2024)

Table 7 - Attacks and arrests by affiliations and number of court cases

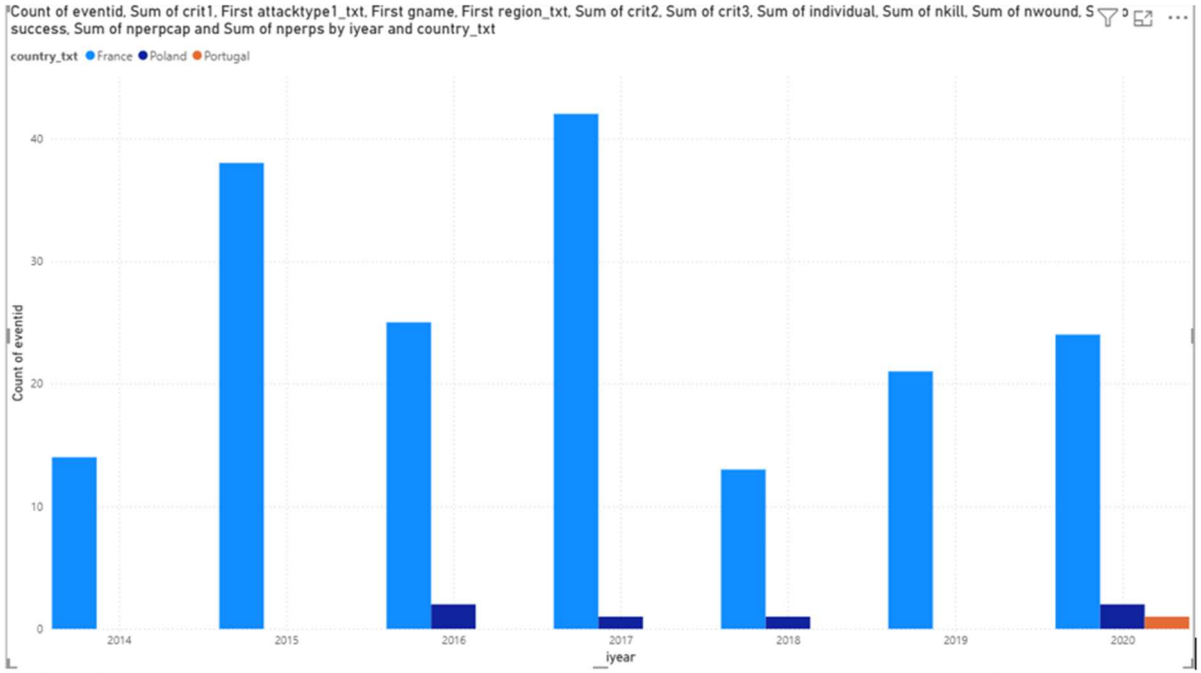
Year	Country	Type	Attacks		Arrests		Court Cases			
			N.º	T	N.º	T	N.º	Convictions	Acquittals	T
2013	PT	All *	0	0	0	0	0	0	0	0
	PL	All *	0	0	0	0	0	0	0	0
	FR	Jihadist	0	63	143	225	20	49	2	51
		Left-Wing	0		1		0			
		Right-Wing	58		3		0			
		Separatist	0		77		29			
		Other	5		1		2			
2015	PT	Separatist **	0	0	2	2	0	0	0	0
	PL	Jihadist **	0	0	4	17	0	0	0	0
		Right-Wing **	0	0	13		0			
	FR	Jihadist	15	73	377	424	5	14	0	14
		Left-Wing	0		1		0			
		Right-Wing	7		2		0			
		Separatist	47		44		9			
		Other	4		0		0			
2017	PT	Jihadist **	1	1	1	1	1	0	1	1
	PL	Jihadist **	0	0	2	2	4	3	1	4
	FR	Jihadist **	11	54	373	411	114	117	5	122
		Left-Wing **	1		10		0			
		Right-Wing **	0		15		0			
		Separatist **	42		13		8			

Year	Country	Typo	Attacks		Arrests		Court Cases			
			N.º	T	N.º	T	N.º	Convictions	Acquittals	T
2014	PT	All *	0	0	0	0	0	0	0	0
	PL	Right-Wing **	0	0	14	14	0	0	0	0
	FR	Jihadist	1	52	188	238	33	35	2	37
		Left-Wing	0		1		0			
		Right-Wing	0		5		1			
		Separatist	50		41		3			
		Other	1		3		0			
2016	PT	Jihadist **	0	0	1	1	1	0	1	1
	PL	Jihadist **	0	0	5	6	0	0	0	0
		Right-Wing **	0		1		0			
	FR	Jihadist **	5	23	429	456	68	68	0	68
		Left-Wing **	0		1		0			
		Separatist **	18		26		0			
2018	PT	All *	0	0	0	0	0	0	0	0
	PL	Other **	0	0	2	2	0	0	0	0
	FR	Jihadist **	10	30	273	310	123	136	5	141
		Left-Wing **	0		3		0			
		Right-Wing **	0		32		0			
		Separatist **	20		2		18			

Year	Country	Type	Attacks		Arrests		Court Cases			
			N.º	T	N.º	T	N.º	Convictions	Acquittals	T
2019	PT	Jihadist **	0	0	1	1	1	1	0	1
	PL	Jihadist **	0	1	2	4	0	0	0	0
		Left-Wing **	1		0		0			
		Right-Wing **	0		2		0			
	FR	Jihadist **	7	14	202	224	89	107	0	107
		Right-Wing **	7		7		0			
		Separatist **	0		13		18			
		Other **	0		2		0			
2020	PT	Jihadist **	0	0	0	1	2	2	0	2
		Left-Wing **	0		1		0			
	PL	Jihadist **	0	0	8	9	0	0	0	0
		Right-Wing **	0		1		0			
	FR	Jihadist **	8	15	99	127	143	149	6	155
		Left-Wing **	1		11		0			
		Right-Wing **	1		5		0			
		Separatist **	5		12		12			
2021	PT	Jihadist **	0	0	2	2	0	0	0	0
	PL	Other **	0	0	3	3	0	0	0	0
	FR	Jihadist	5	5	96	140	83	99	8	107
		Left-Wing	0		3		0			
		Right-Wing	0		29		9			
		Separatist	0		12		6			
		Other	0		0		9			
2022	PT	Jihadist **	0	0	1	1	2	2	0	2
	PL	All *	0	0	0	0	0	0	0	0
	FR	Jihadist **	4	6	93	109	100	103	7	110
		Right-Wing **	2		16		2			
		Separatist **	0		0		8			
2023	PT	All *	0	0	0	0	0	0	0	0
	PL	Jihadist **	0	0	1	1	0	0	0	0
	FR	Jihadist	8	80	62	78	59	73	17	90
		Left-Wing	0		0		1			
		Right-Wing	1		4		17			
		Separatist	70		11		13			
		Other	1		1		0			

Source: Own elaboration based on TE-SAT reports (2014–2024)[87]

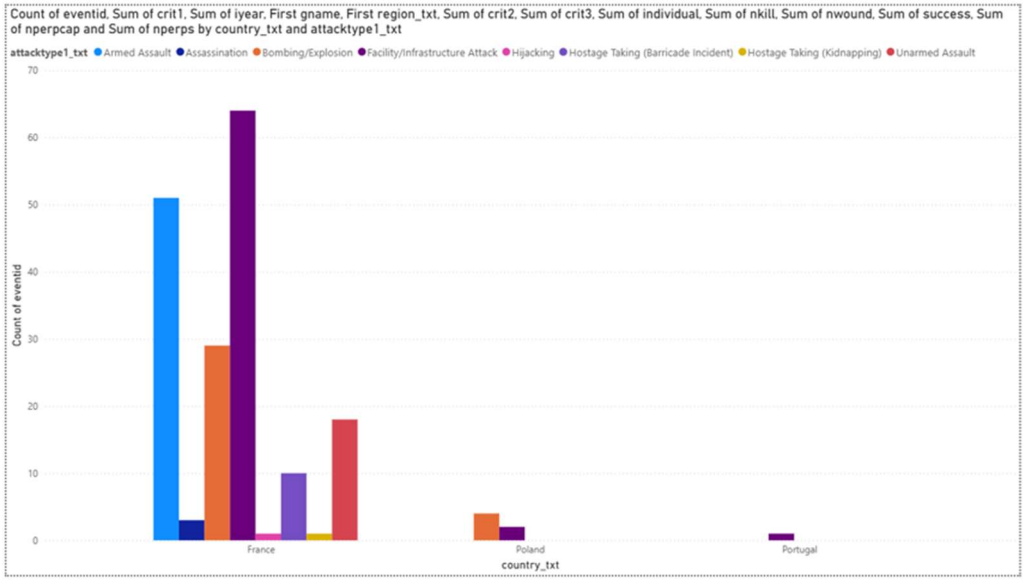
[87] **Legend:** * No records registered regarding the types (Jihadist; Far-Left; Far-Right; Separatist; Other); ** Record(s) only for the type(s) indicated; PT – Portugal; PL – Poland; FR – France; T – Total; N.º – Number.



Year	Country	Count of Events	Attack Type	Group Name	Nmr of Individuals	Nmr of Kills	Nmr of Wounded
2020	Portugal	1	Facility/Infrastructure Atack	Unkown	0	0	0
2016	Poland	2	Bombing/Explosion	Anti-Immigrant Extremists; Anarchists	1	0	1
2014	France	14	Armed Assult;	Animal Liberation Front (ALF)	2	1	15
2015		38	Armed Assult;	Al-Qaeda	6	162	443
2016		25	Armed Assult; Bombing/Explosion;	Anti-Muslim extremists; Anarchists;	8	94	457
2017		42	Armed Assult; Bombing/Explosion;	Anarchists Revolt Against Exiled Gendarmes; Unknown;	11	7	28
2018		13	Armed Assult; Bombing/Explosion;	Animal Rights Extremists; Unknown;	7	13	34
2019		21	Armed Assult;	Anarchists Revolt Against Exiled Gendarmes	6	8	30
2020		24	Armed Assult; Facility/Infrastructure Attack;	Action Directe Anarchiste (ADA); Conspiracy Theory Extremists;	6	11	16

Figure 1 - Number of terrorist attacks by country and by year (2014-2020)

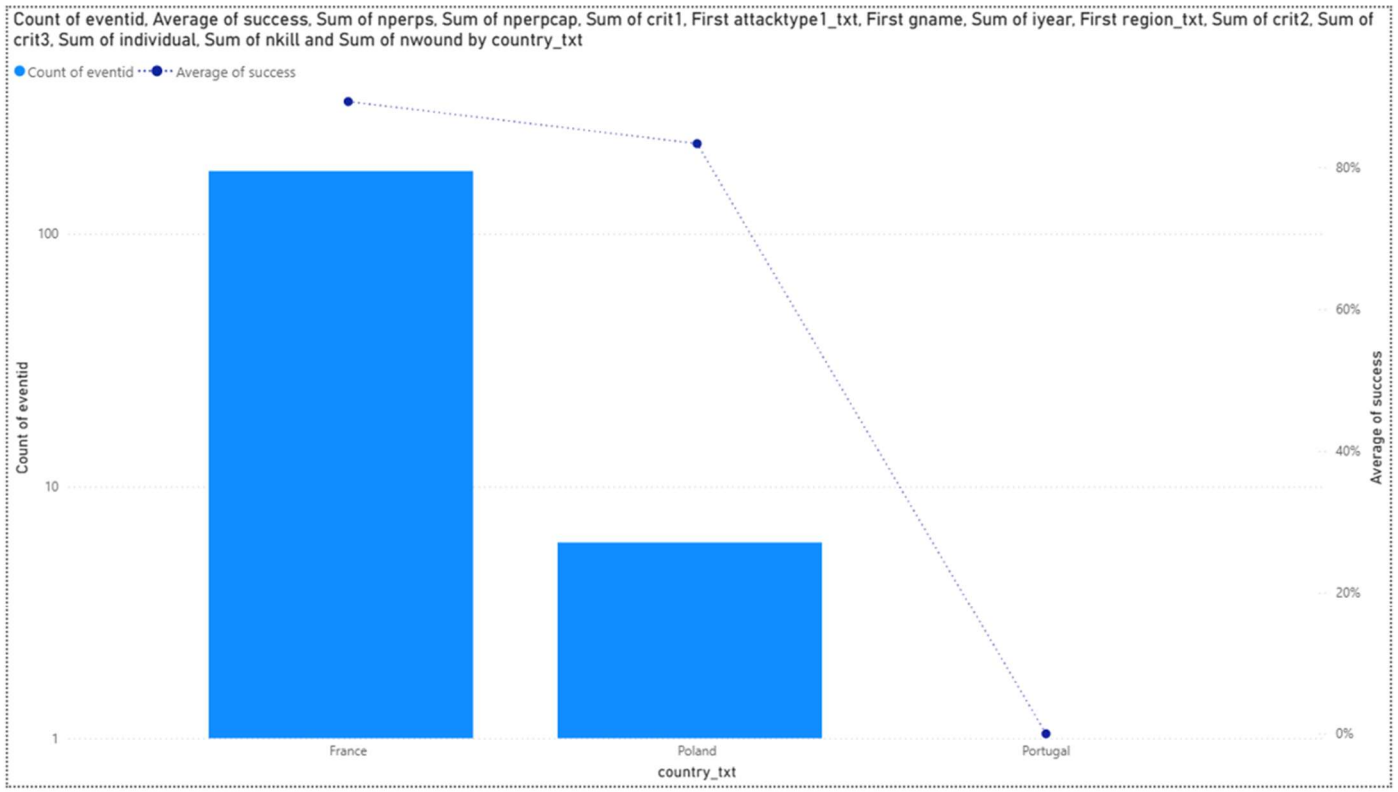
Source: Developed using Power BI based on data from the Global Terrorism Database (2014–2020)



Country	Attack Type	Count of Events	Nmr of Individuals	Nmr of Kills	Nmr of Wounded
Portugal	Unknown	1	0	0	0
Poland	Anarchists	4	1	0	1
	Conspiracy Theory Extremists	2	0	0	0
France	Al-Mahdi	51	28	159	581
	Conspiracy of Cells of Fire	3	1	4	1
	Corsican National Liberation Front (FLNC)	29	2	6	133
	Action Directe Anarchiste (ADA)	64	0	0	1
	Jihadi-Inspired Extremists	1	1	1	1
	Al-Qaeda	10	6	121	252
	Jihadi-Inspired Extremists	1	1	2	0
	Anti-Muslim Extremists	18	7	3	54

Figure 2 - Types of Terrorist Attack and Groups Responsible by Country (2014-2020)

Source: Developed using Power BI based on data from the Global Terrorism Database (2014–2020)



Country	Attack Type	Group Name	Count of Events	Average of Success	Nmr of Individuals	Nmr of Kills	Nmr of Wounded
Portugal	Facility/Infrastructure Attack	Unknown	1	0%	0	0	0
Poland	Bombing/Explosion	Anarchists	6	83%	1	0	1
France	Armed Assault	Action Directe Anarchiste (ADA)	177	89%	46	296	1023

Figure 3 - Total number of attacks, average success rate and human impact by country (2014-2020)

Source: Developed using Power BI based on data from the Global Terrorism Database (2014–2020)

APPENDIX F – METHODOLOGY, METHODS AND MATERIALS

Appendix F.1 – Methodological Approach

The methodological approach adopted in this research follows a qualitative strategy, aligned with the nature and complexity of the phenomenon under investigation (Vilelas, 2020; Patton, 2015). An inductive reasoning method was employed, allowing theoretical generalisations to emerge from the observation of empirical data (Rosado, 2017; Santos & Lima, 2019). Data collection was based on documentary analysis of national and European official documents, academic literature, and institutional reports, complemented by semi-structured interviews designed to enhance data triangulation (Sarmento, 2013). Three Interview Guides (IG A, B, and C) were developed according to the thematic dimensions derived from the research objectives and Derived Questions (DQ), ensuring contextual adequacy and methodological rigour (Gil, 2008; Fortin, 1999; Santos & Lima, 2019).

A cross-sectional research design was adopted, allowing for the collection and analysis of qualitative data at a specific point in time, facilitating the identification of patterns and associations among Portugal, Poland, and France (Santos & Lima, 2019). For further details on the analytical model and interview logistics, see Appendices H and I.

Appendix F.2 – Data Collection Method

Data collection for this study combined two complementary techniques: documentary analysis and semi-structured interviews. Primary data sources included current legislation, official reports, institutional documents and statistical databases such as the GTD, the GTI (2014–2024), Europol's TE-SAT Reports (2014–2024), the Portuguese Internal Security Reports (RASI 2014–2024), and France's *Livre Blanc*[88]. Secondary sources consisted of books, peer-reviewed journal articles, academic dissertations, and relevant grey literature. These were accessed through physical and digital libraries, using systematic searches across academic databases. The sources were organised into four thematic categories, as presented in Appendix H.

[88] *Vide* Appendix H for further explanation.

In addition, semi-structured interviews were conducted with two distinct groups of respondents using different Interview Guides (IGs)[89]. These guides contained pre-established open-ended questions, providing flexibility and allowing for an in-depth exploration of the key themes (Santos & Lima, 2019; Prodanov & Freitas, 2013), thus contributing to the validity of the investigation. Contact with interviewees[90] was established via institutional email or phone and all participants received a Letter of Introduction along with the respective IG prior to the interview. Consent to record the interviews was obtained, with confidentiality guarantees clearly communicated. Most interviews were conducted in person, with two conducted electronically due to professional constraints of the participants (Appendix J). The interviews contributed critical insights to answering the DQ, particularly concerning institutional mechanisms and challenges related to the prevention and combat of Freelance Terrorism in Portugal and Poland[91]. The characterisation of interviewees and the coding and analysis of interview data are detailed in Appendix J.

Appendix F.3 – Data Collection Method

The sampling strategy adopted in this study was based on non-probability methods, specifically a combination of convenience and purposive sampling. This approach was selected due to the qualitative nature of the research, which prioritises the depth and relevance of information over statistical generalisability. According to Rosado (2017), goal-directed sampling is particularly appropriate when the aim is to gather data from individuals with specialised knowledge or direct experience in the research field. The universe targeted by this study included public entities and professionals engaged in counter-terrorism activities in Portugal, Poland and France. From this broader universe, a sample was intentionally selected based on participants' expertise and institutional relevance to the themes of terrorism prevention and combat. The selection criteria focused on ensuring a balance between operational and strategic perspectives.[92]

[89] *Vide* Appendix I – Letter of Introduction in Portuguese, French and English – which contains the letter of introduction, the informed consent protocol, and the interview guides.
[90] *Vide* Appendix H.
[91] The interview surveys were not conducted within the French context, as French authorities officially declined to participate in the research, as per Appendix H.
[92] The universe corresponds to the full set of subjects or observations eligible for inclusion in the study, while the sample represents a deliberately selected portion of that universe (Marconi & Lakatos, 2003).

To facilitate the data collection process, three distinct Interview Guides (IGs) were designed: IG Type A for Portuguese entities, IG Type B for French entities and IG Type C for Polish entities. Each guide was adapted to the specific national context and language, ensuring clarity and relevance for the respondents. A Letter of Introduction was sent to all participants prior to the interviews, explaining the research framework, objectives, and guaranteeing the confidentiality and anonymity of their participation. Interviews were conducted either in person or remotely, depending on the participants' availability. Informed consent was obtained prior to recording the interviews, and all participants were anonymised using randomised coding. This method ensured the protection of personal data and the authenticity of the responses collected.

Despite initial contacts being established with French authorities, participation was officially declined. This limitation is acknowledged in the study and discussed in the final chapter regarding research constraints. Nonetheless, interviews conducted in Portugal and Poland yielded a diverse and methodologically coherent sample, sufficient to meet the research objectives and achieve thematic saturation, as recommended by Sim *et al*. (2018). For the complete list of entities contacted and the characterisation of interviewees, including their professional roles, please refer to Appendix H and J.

Appendix F.4 – Data Processing and Analysis Techniques

The data processing and analysis procedures were based on a qualitative CA approach, which enables the interpretation of respondents' narratives and the identification of patterns and underlying meanings (Charmaz, 2004; Sparkes & Smith, 2014, as cited in Resende, 2016). CA was complemented by quantitative elements, such as the frequency analysis of specific terms and expressions, to reinforce the validity and consistency of thematic patterns (Resende, 2016).

The analysis followed the ITCI method recognised as a robust technique for the treatment of unstructured qualitative data in academic research (Resende, 2016). Initially, the interviews were fully transcribed and organised into question/answer pairs (Guerra, 2006; Resende, 2016), forming the primary corpus for analysis. The subsequent categorisation process entailed iterative reading and the development of a coding framework based on inductive reasoning, ensuring adherence to principles of homogeneity, exclusivity, objectivity and exhaustiveness (Johnson & Christensen, 2014).

The analytical process was operationalised using MAXQDA software, which facilitated efficient data management, generation of coding matrices, cross-referencing, and

systematisation of analytical categories. The methodological steps outlined by Guerra (2006)[93] were strictly followed, including exploratory reading, descriptive analysis, synopsis elaboration and interpretive analysis. The data were reduced and abstracted in accordance with Mayring, (1983) and Flick (2005) (cited in Rodrigues, 2021) principles, allowing the construction of condensed statements that preserve conceptual rigour.

Categories were structured around the DQ and SO, ensuring that the empirical material was systematically aligned with the study's analytical model. Coding was conducted through an alphanumeric system to maintain anonymity and facilitate cross-reference. For the full coding matrices and detailed categorisation schemes, see Appendix J.

[93] Methodological principles defined by Guerra (2006): i) full transcription; ii) exploratory reading; iii) synopsis elaboration; iv) descriptive analysis; v) interpretative analysis.

APPENDIX G – SUPPLEMENTARY INFORMATION ON THE PRESENTATION, ANALYSIS AND DISCUSSION OF RESULTS

Appendix G.1 - Thematic Analysis and Coding Overview (IG Type A)

Table 8 - Coding Scheme Used for Thematic Analysis (IG Type A)

IG Type A	Main Themes	E1	E2	E3	Consensus/ Divergence
1	Institutional roles	Coordination mandate	Strategic intelligence	Operational response	Divergence
2	Conceptualisation	Broader perspective	Ideological individuals/cells	Ideological individuals/cells	Partial consensus
3	Profiling	No extrapolation	Youth online radicalisation	Youth online radicalisation	Partial consensus
4	Risk perception	No conclusion	Digital radicalisation, EU standards	Digital radicalisation, EU standards	Divergence
5	Prevention strategies	ENCT 2023	Intelligence monitoring	OSINT, awareness campaigns	Divergence
6	Tactical responses	Strategic documentation	Intelligence-led operations	Intelligence-led operations, coordination plans	Partial consensus
7	National coordination	Confirmed, technical team	Confirmed, coordination frameworks	Confirmed, restricted plans	Consensus
8	International information exchange	Yes, through Europol	Europol, Counter Terrorism Group	Europol, TE-SAT Reports	Consensus
9	International cooperation	Positive, no concrete protocols	Positive, no concrete protocols	Positive, no concrete protocols	Consensus (no concrete protocols)
10	Legal/procedural challenges	No comment	Acknowledged	Acknowledged	Partial consensus
11	Legislative adequacy	Revision of UCAT decree	Legislation adequate, needs improvements	Reforms for digital threats	Partial consensus
12	Early detection	Recognised	Recognised	Recognised	Consensus
13	Frontline staff involvement	Emphasised frontline agents	Recognised importance	Recognised importance (even off-duty agents)	Consensus
14	HUMINT and OSINT use	No comment	Mentioned HUMINT and OSINT	Mentioned HUMINT and OSINT	Partial consensus
15	AI potential	Recognised, exploratory stage	Recognised, exploratory stage	Recognised, exploratory stage	Consensus
16	Model evaluation	No comment	Effective and adaptable	Effective and adaptable	Partial consensus
17	Preparedness and public involvement	No comment	Supported, need for adaptation	Supported, need for adaptation	Partial consensus
18	Proposals for improvement	Academic involvement positive	Legal revision, training, digital literacy	Legal revision, training, digital literacy, raised alert level	Partial consensus
19	Academic and civil society involvement	Academic involvement positive	Academic involvement positive	No comment	Partial consensus

Appendix G.2 - Thematic Analysis and Coding Overview (IG Type C)

Table 9 - Coding Scheme Used for Thematic Analysis (IG Type C)

IG Type C	Main Themes	E4	E5	Consensus/ Divergence
1	Institutional roles	Tactical response role	Strategic prevention and special operations	Complementary
2	Conceptualisation	Self-radicalised individuals or small groups	Self-radicalised individuals or small groups, absence of structured support	Consensus
3	Profiling	Digital surveillance of isolated individuals	Disguised infiltration, ideological camouflage	Partial convergence
4	Risk perception	Global radicalisation dynamics	Global radicalisation, low-tech tools, online indoctrination	Consensus
5	Prevention strategies	Preparedness	Sensitisation, intelligence-led policing, early intervention	Partial convergence
6	Tactical responses	Tactical response to threats	Tactical response, HUMINT, scenario-based simulations	Partial convergence
7	National coordination	Centralised coordination mechanism	Centralised coordination mechanism	Consensus
8	International information exchange	Europol, Frontex	Europol, Frontex; importance of geography	Consensus
9	International cooperation	General EU cooperation, limited with Portugal	General EU cooperation, potential for bilateral improvement	Consensus (limited bilateral ties)
10	Legal/procedural challenges	Linguistic, legal, procedural discrepancies	Linguistic, legal, procedural discrepancies; digital priorities	Consensus
11	Legislative adequacy	Frameworks adequate	Call for more agile, digitally adaptive procedures	Partial consensus
12	Early detection	Anonymity, low public awareness	Anonymity, encrypted communications, dark web	Consensus
13	Frontline staff involvement	Frontline personnel critical	Frontline personnel critical, community trust	Consensus
14	Intelligence gathering (HUMINT, OSINT, SIGINT)	HUMINT	HUMINT, OSINT, SIGINT, behavioural analysis	Consensus with additional depth (E5)
15	AI potential	AI for predictive analysis	AI for predictive analysis, bias and human supervision concerns	Consensus
16	Model evaluation	Deterrent value of Vigipirate model	Deterrent value, need for socio-political adaptation	Partial consensus
17	Preparedness and public involvement	Adaptation of models	Adaptation of models, culturally sensitive implementation	Partial consensus
18	Proposals for improvement	Early detection, inter-agency coordination	Early detection, coordination, public resilience, deradicalisation, international alignment	Partial consensus
19	Academic and civil society involvement	Officer well-being, public education, digital surveillance cooperation	Hybrid threats, disinformation, community trust-building	Complementary perspectives

Appendix G.3 - Thematic Comparative Analysis and Coding Overview

Table 10 - Thematic Comparative Analysis and Coding Overview

Theme	Q	Portugal	Poland	Main Differences
Institutional Model	Q 1	Segmented roles: strategic coordination, intelligence, operational deployment; reliant on inter-agency coordination	Integrated model: preparedness, response, strategic foresight within elite units	Portugal relies on inter-agency coordination; Poland integrates functions within units
Conceptualisation of Freelance Terrorism	Q 2	Abstract definitions; no recent attack experience	Operationalised profiles; emphasis on border infiltration and refugee dynamics	Portugal's view is more abstract; Poland provides operational profiles
Profiling and Detection Challenges	Q 3 & Q 4	Less operationalised profiles; absence of border infiltration concerns	Detailed detection challenges; attention to refugee routes and decentralised radicalisation	Portugal lacks concern with border issues; Poland highlights them
Preventive Strategies	Q 5	Focus on ENCT, training, and OSINT monitoring	Broader strategies including public engagement and behavioural detection	Portugal follows institutional frameworks; Poland operationalises prevention
Combat Mechanisms	Q 6	Generic references to intelligence-led interventions	Greater use of simulations, HUMINT, scenario-based planning	Portugal is more policy-referential; Poland operationalises simulations and HUMINT
Institutional Coordination	Q 7	Structured national coordination across agencies	Centralised coordination within intervention forces	Both structured, but Poland's system is more centralised
International Cooperation	Q 8 & Q 9	Active participation in Europol and Frontex; limited bilateral ties	Strong participation in Europol, Frontex; noted potential for improving bilateral ties	Similar engagement; Poland seeks enhanced bilateral ties
Challenges and Legal Framework Adequacy	Q 10 and Q 11	Framework considered adequate but requires digital adaptation	Adequate framework; stronger emphasis on agility and digital safeguards	Both adequate; Poland demands more agility
Challenges	Q 12	Challenges in early detection and online anonymity	More nuanced insights into digital radicalisation channels	Similar challenges; Poland offers deeper digital insight
Frontline Staff and Community Engagement	Q 13	Emphasis on frontline vigilance; less focus on community trust	Greater emphasis on community trust and relational intelligence	Portugal stresses vigilance; Poland emphasises community trust
Use of Technology (HUMINT, AI, Digital Tools)	Q 14 & Q 15	Recognition of HUMINT and AI, but limited implementation	Technologically reflective; concerns about AI bias and data protection	Both use HUMINT/AI; Poland shows deeper technological concern
Adoption of Foreign Models (e.g., Plan Vigipirate)	Q 16 & Q 17	Recognition of the need for adaptation, less critical contextualisation	Critical and context-sensitive assessment of foreign models	Portugal less critical; Poland stresses context-sensitive adaptation
Proposals for Improvement	Q 18	Focus on legislative revision, training, and public resilience	Focus on early detection, deradicalisation programmes, and international alignment	Portugal focuses on legal and training aspects; Poland integrates broader resilience strategies
Academic and Civil Society Involvement	Q 19	Recognition of academic involvement; tension with institutional discretion	Greater emphasis on hybrid threats, disinformation, and community trust-building	Portugal values academia but is more reserved; Poland actively promotes civil society engagement

APPENDIX H – METHODOLOGICAL FRAMEWORK

Table 11 - Analytical model

General Objective	Specific Objectives	Central Research Question	Derived Questions	Key Concepts	Dimensions of Analysis	Data	
						Data Collection Instruments	Data Analysis Technique
GO – To study the phenomenon of Freelance Terrorism, understanding the methods of prevention and counteraction it in Portugal, based on the case studies of Poland and France.	**SO 1 –** To understand the best way to investigate Freelance Terrorism in Portugal.	**CRQ -** How can Freelance Terrorism be best prevented and countered in Portugal, based on the case studies of Poland and France?	**DQ 1 -** How can Freelance Terrorism be best investigated in Portugal?	- Freelance Terrorism; - Prevention; - Radicalisation; - National Security; - International Cooperation;	- Conceptual; - Legal; - Institutional; - International/ Comparative;	Semi-structured Interviews & Documental Research	Content Analysis & Documental Analysis
	SO 2 - To understand the best way to investigate Freelance Terrorism in Poland.		**DQ 2 -** How can Freelance Terrorism be best investigated in Poland?				
	SO 3 - To understand the best way to investigate Freelance Terrorism in France.		**DQ 3 -** How can Freelance Terrorism be best investigated in France?				
	SO 4 - To understand the best way to prevent Freelance Terrorism in Portugal.		**DQ 4 -** How can Freelance Terrorism be best prevented in Portugal?		- Conceptual; - Legal; - Strategic; - Technological;		
	SO 5 - To understand the best way to prevent Freelance Terrorism in Poland.		**DQ 5 -** How can Freelance Terrorism be best prevented in Poland?				
	SO 6 – To understand the best way to prevent Freelance Terrorism in France.		**DQ 6 -** How can Freelance Terrorism be best prevented in France?		- International/ Comparative;		

Table 12 - Summary of the relationship between interview questions and derived research questions

Derived Questions						Interview Questions			Category	SubCategory
DQ1	DQ2	DQ3	DQ4	DQ5	DQ6	Interview Guide Type A	Interview Guide Type B	Interview Guide Type C		
X	X	X	X	X	X	**1** - Role of the institution in counter-terrorism efforts in Portugal	**1** - Role of the institution in counter-terrorism efforts in France	**1** - Role of the institution in counter-terrorism efforts in Poland	**Institutional Structure**	Responsibilities and Actions
X	X	X	X	X	X	**2** - Definition and characterisation of Freelance Terrorism	**2** - Definition and characterisation of Freelance Terrorism	**2** - Definition and characterisation of Freelance Terrorism	**Concept**	Typology and Framework
X	X	X	X	X	X	**3** - Profiles of freelance terrorists in Portugal	**3** - Profiles of freelance terrorists in France	**3** - Profiles of freelance terrorists in Poland	**Phenomenon Characterisation**	Profiles and Behaviours
X	X	X	X	X	X	**4** - Growth of the phenomenon in Portugal	**4** - Growth of the phenomenon in France	**4** - Growth of the phenomenon in Poland		
\	\	\	X	X	X	**5** - Prevention strategies	**5** - Prevention strategies	**5** - Prevention strategies	**Prevention Mechanisms**	National Strategies
X	X	X	X	X	X	**6** - Combat strategies	**6** - Combat strategies	**6** - Combat strategies	**Combat Mechanisms**	
X	X	X	\	\	\	**7** - National interinstitutional coordination	**7** - Coordination among French entities	**7** - Coordination among Polish entities	**Interinstitutionality**	Internal Cooperation
X	X	X	\	\	\	**8** - Information sharing with European entities	**8** - Information sharing with European entities	**8** - Information sharing with European entities	**International Cooperation**	Information Sharing and Protocols
X	X	X	X	X	X	**9** - Portugal-France (and EU) cooperation in counter-terrorism	**9** - International cooperation, focusing on Portugal	**9** - International cooperation, focusing on Portugal		
X	X	X	X	X	X	**10** - Challenges in international cooperation	**10** - Challenges in international cooperation	**10** - Challenges in international cooperation		
X	X	X	\	\	\	**11** - Adequacy of current legislation	**11** - Adequacy of current legislation	**11** - Adequacy of current legislation	**Legal Framework**	Need for Reforms
X	X	X	X	X	X	**12** - Main challenges faced	**12** - Main challenges faced	**12** - Main challenges faced	**Operational Challenges**	Practical Limitations
X	X	X	X	X	X	**13** - Role of the individual actor	**13** - Role of the individual actor	**13** - Role of the individual actor	**Individual Capacities**	Responsibility and Initiative
\	\	\	X	X	X	**14** - Importance of HUMINT and other methods	**14** - Importance of HUMINT and other methods	**14** - Importance of HUMINT and other methods		
X	X	X	\	\	\	**15** - Use of Artificial Intelligence	**15** - Use of Artificial Intelligence	**15** - Use of Artificial Intelligence	**Artificial Intelligence**	Methods and Limitations
X	\	X	X	\	X	**16** - pinion on the French *Plan Vigipirate*	**16** - pinion on the French *Plan Vigipirate*	**16** - pinion on the French *Plan Vigipirate*	**Comparative Models**	Good Practice Transfers
X	\	X	X	\	X	**17** - Possible implementation of a similar plan in Portugal	**17 -** Adaptation of the *Plan Vigipirate* to other countries (especially Portugal)	**17 -** Adaptation of the *Plan Vigipirate* to other countries (especially Portugal)		
X	X	X	X	X	X	**18** - Recommendations for improvement	**18** - Recommendations for improvement	**18** - Recommendations for improvement	**Suggestions**	Measures and Enhancements
X	X	X	X	X	X	**19** - Additional relevant issues	**19** - Additional relevant issues	**19** - Additional relevant issues	**Open Insights**	Additional Perspectives

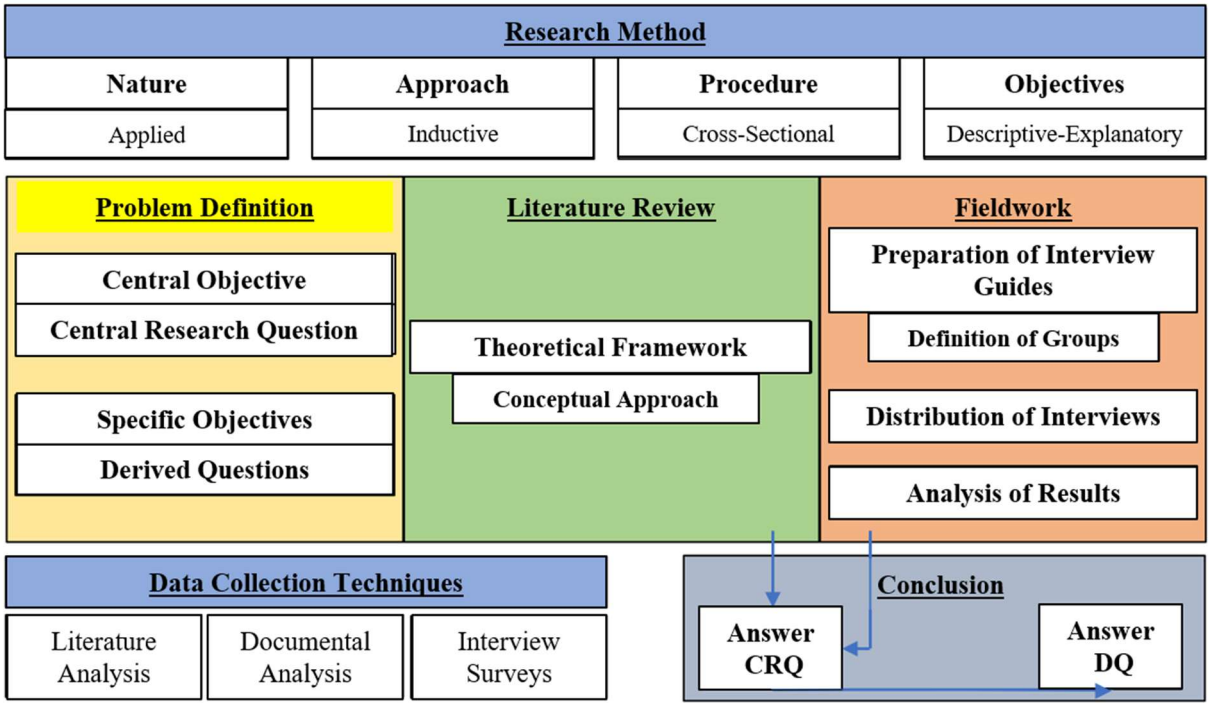


Figure 4 - Diagram of the Investigation Design

This research has opted to use the TE-SAT reports from Europol as the primary source of data on terrorist incidents and counterterrorism activities, given the need for a comparative approach. This decision was made in preference to the Portuguese RASI reports and the French *Livre Blanc* (there are no Polish national reports), which are used as complementary sources, for the following reasons:

Table 13 - Comparison between Europol TE-SAT Reports and Portuguese, Polish and French National Reports

Criteria	TE-SAT Reports (Europol)	RASI	*Livre Blanc*
Geographic scope	European Union	Portugal	France
Periodicity and structure	Annual, with standardised thematic sections	Annual, without a dedicated section on terrorism	Irregular publication; broad strategic focus; no dedicated terrorism section
Type of data	Quantitative and qualitative; attacks, arrests, trends	Summary, descriptive; little analytical depth	Descriptive and strategic; lacks quantitative terrorism-specific indicators
International comparability	High (enables comparative analysis between countries)	Low (focus exclusively on national context)	Low (not designed for cross-country terrorism comparison)

Thematic specificity	Terrorism Freelance; Jihadism; other ideological extremisms	Mentions terrorism, but with limited detail	Mentions terrorism in general; limited focus on freelance or decentralised threats

TE-SAT: The TE-SAT (Terrorism Situation and Trend Reports) published by Europol offer a detailed, both quantitative and qualitative, analysis of terrorism within the European Union, enabling a more robust comparison between Member States. These reports highlight essential data such as: i) the number of terrorist attacks recorded in the EU (failed, foiled, and completed); ii) predominant modus operandi, including the rise of freelance terrorism and the methods used (knives, vehicles, improvised explosive devices); iii) the number of terrorism-related arrests in each Member State, allowing for an assessment of the intensity of the threat across countries; iv) trends in online radicalisation, including the role of social media and mass communication platforms in spreading extremist propaganda.

RASI: It is important to note that although the RASI reports provide information on the terrorist threat in Portugal, their scope is limited, as they focus exclusively on national territory and address terrorism in a non-systematic manner. Given Portugal's history of low risk, the analysis of terrorism in the RASI tends to be brief and lacks depth, mainly concentrating on international cooperation and the monitoring of suspected individuals.

Lack of Polish Report: Although certain governmental communications and institutional briefings address terrorism-related matters, there is no unified, periodic document that systematises data in a way that enables cross-national comparison. The available information is often fragmented across different ministries or agencies, lacking thematic depth or consistent structure. Consequently, while Poland represents a valuable case study at the operational and institutional level (particularly through entities such as the ABW and TPCE), its documentary sources cannot serve as a robust basis for quantitative or thematic comparison.

Livre Blanc: The French *Livre Blanc* on defence and national security occasionally includes considerations related to terrorism, but does so within a broader strategic framework rather than in a focused or recurring manner. Its last full edition dates back several years (2006), and while it outlines France's general security posture, it lacks standardised indicators or quantitative metrics specific to terrorism. Furthermore, the *Livre Blanc* does not offer sufficient granularity regarding phenomena such as freelance terrorism or digital

radicalisation, which are central to this dissertation. Therefore, despite France's central role in European counterterrorism, the *Livre Blanc* is more suitable as a contextual or complementary source than as a primary reference.

Conclusion: Given the need for structured, comparative, and thematically specific data, the TE-SAT reports from Europol were selected as the primary source of empirical reference in this dissertation. Their regularity, analytical depth, and comparability across Member States offer a solid empirical basis for understanding the evolution and nature of terrorism within the EU, especially regarding decentralised threats such as Freelance Terrorism. National reports, while valuable for contextual insight, remain supplementary due to their limited scope, heterogeneity, and varying degrees of analytical robustness.

Table 14 - Overview of the types of databases and repositories consulted

Category	Platform/Repository	Type of Content
Institutional Repositories	RCAAP; PubMed	Master's Dissertations; Doctoral Theses; Technical and Scientific Reports
Academic Databases	EBSCO; JSTOR; CAIRN; Google *Scholar*	Scientific Articles; Conference Papers
Scientific Sharing Networks	ResearchGate	Empirical Studies; Communication among Researchers
Specialised Legal Platforms	DATAJURIS; EUR-Lex	European and National Legislation; Directives; Regulations; Legal Opinions

The selection of sources was based on criteria of topicality, thematic relevance, peer review, and indexing in recognised databases. The key terms used included: "Terrorism", "Freelance Terrorism", "Radicalisation", "Terrorism Prevention", "Counterterrorism", "Antiterrorism", and "International Cooperation".

Regarding the entities contacted within the scope of the sampling process, it is important to note some aspects. At the national level, not all entities with differentiated responsibilities within the national security system agreed to participate in the study. The OSCOT, due to its scientific relevance in the analysis of this issue, was among the few that accepted to collaborate and respond to the semi-structured interview, which resulted in a smaller sample than initially anticipated. When the directors of UNCT and OSCOT were contacted by the means mentioned in the table below, they initially affirmed and confirmed their collaboration with the study. However, after several attempts to persuade them to do

so, no response was received, nor was any justification given. As a result, the previously agreed collaboration with these organisations was not achieved, making it impossible to collect the results needed for this study.

Regarding Poland, the contacts were made possible with the support of the assistant-supervisor, (PhD) Monika Wysocka, who facilitated connections with entities and professionals holding responsibilities in the field of counterterrorism. The interviews conducted in Poland provided relevant data for the comparative component of this study.

In the case of France, formal contact was established with the support of the *Divisão de Planeamento Estratégico e Relações Internacionais* (DPERI) of the Portuguese *Guarda Nacional Republicana*, which liaised with the French Embassy in Portugal, and directly by the Researcher. Despite having submitted all institutional documents and the interview guides, the French authorities formally declined participation via e-mail, citing internal guidelines. This constituted a limitation of the present research.

Table 15 - Contacted Entities

	Entity	Sub-Entity	Means of Contact	Response
PT	GNR	*Comando Operacional* (CO)	E-mail	Forwarded
		Comando da Administração dos Recursos Internos (CARI)	E-mail	Forwarded
		Comando de Doutrina e Formação (CDF)	E-mail	Forwarded
		Direção de Informações (DI)	E-mail, Telephone and In-Person	Participated and responded
		Direção de Investigação Criminal (DIC)	E-mail and Telephone	Participated
		GIOE	E-mail and Telephone	Participated
	PJ	UNCT	E-mail, Telephone and In-Person	Participated but Never Responded ***
	SIRP	\	E-mail	Participated and responded
		SIS	E-mail	Participated and responded
		SIED	E-mail	Refused **
	SSI	UCAT	E-mail, Telephone and In-Person	Participated and responded
	Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT)	\	E-mail and Telephone	Participated but Never Responded ***
PL	GROM	\	Through the Assistant-Supervisor and E-mail	Participated and responded
	FORMOZA	\	Through the Assistant-Supervisor and E-mail	Participated and responded
	ABW	\	Through the Assistant-Supervisor and E-mail	Participated but Never Responded ***
FR	\	\	*Via* Embassy *	Refused

Legend: * Contacted *via* the *Divisão de Planeamento Estratégico e Relações Internacionais* (DPERI) of the Portuguese *Guarda Nacional Republicana* (GNR), and by the Researcher;
**** Declined to participate, citing institutional confidentiality considerations; *** They were contacted in good time, confirmed their collaboration by telephone and/or in-person, but did not materialise it and did not give reasons to why.**

APPENDIX I – LETTER OF INTRODUCTION

GUIÃO DE ENTREVISTA TIPO A

ACADEMIA MILITAR

O Terrorismo Freelance, formas de prevenção e combate:
Estudo comparativo entre Portugal, Polónia e França

Autor: Aspirante GNR Infantaria Diogo dos Santos Almeida

Orientador: Tenente-Coronel GNR Infantaria (Doutor) Tiago Gonçalves Silva

Coorientador: (Doutora) Monika Wysocka

Mestrado Integrado de Ciências Militares na Especialidade de Segurança
Dissertação de Mestrado
Lisboa, junho 2025

Figure 5 - Letter of Introduction in Portuguese 1/7

CARTA DE APRESENTAÇÃO

No âmbito do ciclo de estudos do Mestrado Integrado em Ciências Militares, os alunos da Academia Militar desenvolvem uma dissertação final denominada de Trabalho de Investigação Aplicada (TIA), requisito para a obtenção do grau de mestre. O TIA é submetido a apreciação e discussão pública perante um júri com o objetivo da aplicação das competências adquiridas, desenvolvimento de capacidades e exposição das conclusões nos domínios da Segurança e Defesa. No presente ano letivo, é pretendido que os futuros oficiais desenvolvam a investigação no sentido de apresentar conclusões sobre o tema de "A Prevenção Criminal e os Modelos de Policiamento".

A investigação tem como objetivo principal analisar as estratégias de prevenção e combate do fenómeno de Terrorismo, em particular o Terrorismo Freelance, em Portugal, utilizando o estudo de caso da Polónia e da França. Pretendo identificar as práticas mais eficazes de investigação e prevenção adotadas pelas entidades competentes em ambos os países, contribuindo para uma melhor compreensão e resposta ao fenómeno. Deste modo, tendo em conta a abrangência do tema, considero essencial recolher contributos de especialistas na área, razão pela qual solicito, com a presente carta, a colaboração de V. Ex.ª, mediante a realização de uma entrevista. Esta entrevista será fundamental para aprofundar a análise sobre os métodos de investigação, tipos de práticas comuns, prevenção e combate ao Terrorismo, em particular ao Terrorismo Freelance, permitindo-me alcançar os objetivos propostos com rigor e qualidade científica.

Reitero que todos os dados fornecidos serão utilizados única e exclusivamente para fins académicos e no estrito cumprimento das normas de confidencialidade e ética científica.

Desde já, manifesto o meu mais profundo agradecimento pela disponibilidade e atenção demonstrada em apoiar este estudo. A sua colaboração será de inestimável valor para o sucesso da investigação e para o seu contributo ao conhecimento científico.

Atenciosamente,

Diogo dos Santos Almeida

Aspirante de Infantaria da Guarda Nacional Republicana

Figure 6 - Letter of Introduction in Portuguese 2/7

PROTOCOLO DE CONSENTIMENTO INFORMADO

O presente protocolo é estabelecido entre Diogo dos Santos Almeida, aluno da Academia Militar a realizar uma investigação com o tema "*Freelance Terrorism, methods of prevention and combat: A comparative study between Portugal, Poland and France*", e o participante_____,
através do método de entrevista.

O investigador e o orientador científico comprometem-se a:

a) Conduzir a investigação de acordo com os parâmetros de qualidade preconizados pela comunidade científica da especialidade;

b) Discutir e negociar outros aspetos específicos de cada caso relativos à confidencialidade da informação, se solicitado pelo participante;

c) Impedir qualquer divulgação de informação referente aos participantes, exteriormente à equipa de investigação, sem o consentimento prévio de todos os envolvidos;

d) Entregar uma síntese descritiva dos resultados aos participantes, através de correio eletrónico;

e) Manter os participantes a par do trabalho que está a ser desenvolvido, nomeadamente no que concerne à análise dos dados, sempre que os mesmos o solicitem;

f) Prestar aos participantes no processo todos os esclarecimentos solicitados no decorrer da investigação;

g) Cumprir o Código Deontológico da *American Psychological Association* (APA 7.ª edição) na realização da investigação;

h) Eliminar todas as gravações áudio após o decorrer da investigação e a defesa pública da tese.

Os participantes comprometem-se a:

a) Prestar informações sobre a sua experiência no caso em estudo e sobre a sua experiência profissional;

b) Ser entrevistado num momento acordado entre o investigador e o participante;

c) Autorizar a gravação áudio da entrevista, a pedido do investigador;

d) Decidir mencionar ou omitir a sua participação no projeto nos contextos profissionais em que considere conveniente fazê-lo;

Figure 7 - Letter of Introduction in Portuguese 3/7

e) Permitir a publicação do resultado do estudo, com omissão da sua identidade, nomeadamente nas seguintes situações:

I. Tese de Mestrado a apresentar à Academia Militar;

II. Comunicações em congressos científicos-profissionais;

III. Publicações científicas em revistas e/ou em livros da especialidade.

Assinaturas:

_____

(Participante)

_____

(Investigador)

Local e Data:

_____

Figure 8 - Letter of Introduction in Portuguese 4/7

IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	**Hora (Início/Fim):**
U/E/O:	**Data:**
Função/Posto:	**Local:**

ENTREVISTA

As respostas de Sua Excelência são fundamentais para atingir os objetivos da investigação, pelo que se solicita que as mesmas sejam o mais completas possível. As suas respostas irão servir única e exclusivamente como objeto de estudo para a investigação, pelo que lhe é solicitada autorização para efetuar gravação e posterior análise e transcrição das respostas, na certeza, porém que as mesmas serão apagadas como previsto no protocolo. Se for sua intenção, as resposta ser-lhe-ão facultadas, juntamente com o trabalho final, assim que o mesmo seja aprovado.

Questão 1 – Qual o papel da sua instituição no combate ao terrorismo em Portugal?

Questão 2 – Para a sua instituição, como define e caracteriza o terrorismo freelance?

Questão 3 – Quais são os principais perfis de terroristas freelance? E quais os identificados em Portugal?

Questão 4 – Considera que esta forma de terrorismo está a aumentar no contexto português? Porquê?

Questão 5 – Quais são as principais estratégias da sua instituição na prevenção ao terrorismo freelance?

Questão 6 – Quais são as principais estratégias da sua entidade no combate ao terrorismo freelance?

Figure 9 - Letter of Introduction in Portuguese 5/7

Questão 7 – Como se processa a coordenação entre as diferentes instituição portuguesas no combate a esta ameaça?

Questão 8 – Existe partilha de informações com outras organizações europeias? Que tipo de informações são partilhadas?

Questão 9 – Como avalia a colaboração entre Portugal e outros países europeus no combate ao terrorismo? E em particular com a França, como avalia essa colaboração e que protocolos específicos existem?

Questão 10 – Quais os desafios que surgem na colaboração internacional no combate ao terrorismo freelance? E em particular com a França?

Questão 11 – A legislação atual é suficiente para combater esta ameaça ou seriam necessárias reformas?

Questão 12 – Quais são os principais desafios enfrentados na luta contra o terrorismo freelance em Portugal?

Questão 13 – Qual é o papel do agente individual no combate ao terrorismo freelance? Considera que a atuação individual de um agente dentro do sistema de segurança é relevante para o combate ao terrorismo freelance?

Questão 14 – Como avalia a importância da HUMINT (Inteligência Humana) na deteção e prevenção de ameaças terroristas freelance? Que outros métodos de recolha de informação são utilizados pela sua entidade e quais os seus desafios?

Questão 15 – De que forma a inteligência artificial pode ser utilizada como apoio às estratégias de combate ao terrorismo freelance e quais os seus desafios? Existem aplicações concretas já implementadas em Portugal?

Figure 10 - Letter of Introduction in Portuguese 6/7

Questão 16 – Qual é a sua opinião sobre o Plano Vigipirate francês enquanto estratégia nacional de prevenção e combate ao terrorismo? Considera que as medidas implementadas pela França através deste plano são eficazes na luta contra o terrorismo, em particular contra o terrorismo freelance?

Questão 17 – Considera que Portugal beneficiaria da criação de um plano semelhante ao Vigipirate? Que desafios e vantagens antevê na implementação de um sistema desse género no contexto nacional?

Questão 18 – Que recomendações faria para melhorar a prevenção e o combate ao terrorismo freelance em Portugal?

Questão 19 – Identifica algum outro ponto que considere relevante abordar?

Agradeço a sua cooperação.

Figure 11 - Letter of Introduction in Portuguese 7/7

MANUEL D'INTERVIEW TYPE B

ACADÉMIE MILITAIRE

Le Terrorisme Freelance, formes de prévention et de lutte :
Étude comparative entre le Portugal, la Pologne et la France

Auteur : Aspirant GNR Infanterie Diogo dos Santos Almeida

Directeur : Lieutenant-Colonel GNR Infanterie (Docteur) Tiago Gonçalves Silva

Co-directrice : (Docteure) Monika Wysocka

Master Intégré en Sciences Militaires, spécialité Sécurité
Mémoire de Master
Lisbonne, Juin 2025

Figure 12 - Letter of Introduction in French 1/7

LETTRE DE PRÉSENTATION

Au sein des études du Master Intégré en Sciences Militaires, les étudiants de l'Académie Militaire développent un mémoire final, dénommé Travail de Recherche Appliquée (TRA), une exigence pour l'obtention du diplôme de master. Ce travail fait l'objet d'une évaluation et d'une discussion publique devant un jury, visant à appliquer les compétences acquises, à développer des capacités et à exposer les conclusions dans les domaines de la Sécurité et de la Défense. Pour l'année académique en cours, il est attendu que les futurs officiers mènent des recherches visant à présenter des conclusions sur le thème de « La Prévention Criminelle et les Modèles de Police ».

L'objectif principal de cette recherche est d'analyser les stratégies de prévention et de lutte contre le phénomène du Terrorisme, en particulier le Terrorisme Freelance, au Portugal, en prenant comme étude de cas la Pologne et la France. Je souhaite identifier les pratiques d'investigation et de prévention les plus efficaces adoptées par les autorités compétentes dans les deux pays, afin de contribuer à une meilleure compréhension et réponse au phénomène. En raison de l'importance du sujet, il est nécessaire de recueillir les contributions des experts dans le domaine, raison pour laquelle je demande votre collaboration par le biais d'un entretien. Cet entretien sera fondamental pour mieux comprendre les pratiques communes associées aux méthodes d'investigation, de prévention et de lutte contre le phénomène du Terrorisme, en particulier le Terrorisme Freelance.

Je tiens à préciser que toutes les données fournies seront exclusivement utilisées à des fins académiques, dans le strict respect des normes de confidentialité et de l'éthique scientifique.

Je vous remercie d'avance pour l'attention et le soutien que vous porterez à cette demande. La collaboration de votre organisme sera d'une valeur inestimable pour le succès de cette recherche et pour sa contribution au développement des connaissances dans le domaine de la Sécurité et de la Defense.

Respectueusement,

Diogo dos Santos Almeida

Aspirant d'Infanterie de la *Guarda Nacional Republicana*

Figure 13 - Letter of Introduction in French 2/7

ACCORD DE CONSENTEMENT ÉCLAIRÉ

Le présent accord est établi entre Diogo dos Santos Almeida, étudiant de l'Académie Militaire dans le cadre de la conduite d'une enquête sur le thème « *Freelance Terrorism, methods of prevention and combat: A comparative study between Portugal, Poland and France* », et le participant _____, dans le cadre d'une entrevue.

Le chercheur et le directeur de recherche s'engagent à :

a) Mener la recherche en respectant les standards de qualité définis par la communauté scientifique spécialisée ;

b) Discuter et convenir d'autres aspects spécifiques à chaque cas concernant la confidentialité des informations, si le participant en fait la demande ;

c) Garantir la non-divulgation des informations relatives aux participants, à l'extérieur de l'équipe de recherche, sans le consentement préalable des personnes concernées ;

d) Fournir aux participants une synthèse descriptive des résultats par courrier électronique ;

e) Informer les participants de l'avancement des travaux, notamment en ce qui concerne l'analyse des données, sur demande de leur part ;

f) Répondre aux questions des participants et fournir toutes les clarifications nécessaires au cours de l'enquête ;

g) Respecter les principes éthiques définis par le Code de Déontologie de L'*American Psychological Asszociation* (APA, 7e édition) dans la conduite de cette recherche ;

h) Détruire tous les enregistrements audios après la conclusion de l'enquête et la défense publique du Travail de Recherche Appliquée.

Les participants s'engagent à :

a) Fournir des informations sur leur expérience en lien avec l'objet de l'étude ainsi que sur leur expérience professionnelle ;

b) Participer à une interview à une date et une heure convenue avec le chercheur ;

c) Autoriser l'enregistrement audio de l'interview, sur demande du chercheur ;

d) Décider librement de mentionner ou d'omettre leur participation au projet dans leur cadre professionnel, selon leur convenance ;

Figure 14 - Letter of Introduction in French 3/7

e) Autoriser la publication des résultats de l'étude, sous réserve de l'anonymisation de leur identité, notamment dans les cadres suivants :

I. La Thèse de Maîtrise à présenter à l'Académie Militaire ;

II. Des communications lors de congrès scientifiques et professionnels ;

III. Des publications scientifiques dans des revues et/ou livres spécialisés.

Signatures :

_____

(Participant)

_____

(Chercheur)

Lieu et Date :

_____

Figure 15 - Letter of Introduction in French 4/7

IDENTIFICATION DE L'ENQUÊTÉ

Nom :	**Heure (Début/Fin) :**
U/E/O :	**Date :**
Fonction/Poste :	**Lieu :**

INTERVIEW

Les réponses de Votre Excellence sont essentielles pour atteindre les objectifs de cette enquête. Il est donc demandé qu'elles soient aussi complètes que possible. Vos réponses seront utilisées uniquement et exclusivement à des fins de recherche. Ainsi nous sollicitons votre autorisation pour procéder à leur enregistrement, à leur analyse ultérieure ainsi qu'à leur transcription, tout en vous garantissant qu'elles seront effacées conformément aux dispositions prévues dans l'accord. Si vous le souhaitez, vos réponses pourront vous être communiquées avec le travail final dès son approbation.

Question 1 – Quel rôle joue votre institution dans la lutte contre le terrorisme en France ?

Question 2 – Comment votre institution définit-elle et caractérise-t-elle le terrorisme freelance ?

Question 3 – Quels sont les profils principaux de terroristes freelance ? Et ceux identifiés en France ?

Question 4 – Estimez-vous que cette forme de terrorisme connaît une augmentation dans le contexte français ? Pourquoi ?

Question 5 – Quelles sont les principales stratégies mises en place par votre institution pour prévenir le terrorisme freelance ?

Question 6 – Quelles sont les principales stratégies mise en place par votre institution pour combattre le terrorisme freelance ?

Figure 16 - Letter of Introduction in French 5/7

Question 7 – Comment s'organise la coordination entre les différentes entités françaises pour lutter contre cette menace ?

Question 8 – Y a-t-il un partage des informations effectif avec d'autres organisations européennes ? Quel est le rôle de ce partage ?

Question 9 – Comment évaluez-vous la collaboration entre la France et d'autres pays européens dans la lutte contre le terrorisme ? Et en particulier avec le Portugal, comment évaluez-vous cette collaboration et quels sont les protocoles spécifiques ? En particulier avec la GNR (Garde Nationale Républicaine de Portugal) ?

Question 10 – Quels sont les défis qui se posent dans la coopération internationale pour combattre le terrorisme freelance ? Et en particulier avec le Portugal ?

Question 11 – Est-ce que la législation actuelle est adaptée pour faire face à cette menace, ou bien des réformes s'avèrent-elles nécessaires ?

Question 12 – Quels sont les principaux défis auxquels vous faites face dans la lutte contre le terrorisme freelance en France ?

Question 13 – Quel est le rôle de l'agent individuel dans la lutte contre le terrorisme freelance ? Considérez-vous que l'action individuelle d'un agent au sein du système de sécurité est pertinente pour lutter contre le terrorisme freelance ?

Question 14 – Comment évaluez-vous l'importance du HUMINT (Renseignement Humain) dans la détection et la prévention des menaces terroristes freelance ? Quels autres moyens de collecte d'informations sont utilisés par votre organisation et quels sont leurs défis ?

Question 15 – De quelle manière l'intelligence artificielle peut-elle être utilisée pour soutenir les stratégies de lutte contre le terrorisme freelance et quels sont ses défis ? Existe-t-il des applications concrètes déjà mises en œuvre en France ?

Figure 17 - Letter of Introduction in French 6/7

Question 16 – Quel est votre avis sur le Plan Vigipirate en tant que stratégie nationale de lutte contre le terrorisme ? Pensez-vous qu'il s'agit d'un dispositif efficace et pertinent, ou estimez-vous qu'il nécessiterait des améliorations ?

Question 17 – Considérez-vous que d'autres pays, notamment le Portugal, gagneraient à mettre en place un plan similaire au Plan Vigipirate ? Quels seraient, selon vous, les avantages et les défis d'une telle initiative dans un contexte différent ?

Question 18 – Quelles recommandations feriez-vous pour améliorer la prévention et la lutte contre le terrorisme freelance en France ?

Question 19 – Y a-t-il d'autres points que vous considérez essentiels à aborder ?

Je vous remercie de votre coopération.

Figure 18 - Letter of Introduction in French 7/7

INTERVIEW SCRIPT – TYPE C

MILITARY ACADEMY

Freelance Terrorism, ways of preventing and combating it: A comparative study between Portugal, Poland and France

Author: Aspirant GNR Infantry Diogo dos Santos Almeida

Supervisor: Lieutenant-Colonel GNR Infantry (PhD) Tiago Gonçalves Silva

Assistant Supervisor: (PhD) Monika Wysocka

Integrated Master's Degree in Military Sciences, Specialty of Security

Master's Dissertation

Lisbon, June 2025

Figure 19 - Letter of Introduction in English 1/7

PRESENTATION LETTER

As part of the Integrated Master's programme in Military Sciences, students at the Military Academy develop a final dissertation called an Applied Research Paper (ARP), which is a requirement for obtaining a master's degree. The ARP is submitted for public assessment and discussion before a jury with the aim of applying acquired skills, developing capabilities and presenting conclusions in the fields of Security and Defence. In the current academic year, future officers are expected to carry out research in order to present conclusions on the subject of "Crime Prevention and Policing Models".

The main aim of the research is to analyse strategies for preventing and combating the phenomenon of terrorism, particularly freelance terrorism, in Portugal, using the case study of Poland and France. I intend to identify the most effective investigation and prevention practices adopted by the competent authorities in both countries, contributing to a better understanding of and response to the phenomenon. Therefore, given the scope of the topic, I believe it is essential to gather contributions from experts in the field, which is why I am requesting your co-operation with this letter by conducting an interview. This interview will be essential to deepen the analysis of investigation methods, types of common practices, prevention and combating terrorism, in particular freelance terrorism, allowing me to achieve the proposed objectives with rigour and scientific quality.

I reiterate that all the data provided will be used solely and exclusively for academic purposes and in strict compliance with the rules of confidentiality and scientific ethics.

I would like to express my deepest gratitude for your willingness and attention in supporting this study. Your co-operation will be invaluable to the success of the research and your contribution to scientific knowledge.

Yours sincerely,

Diogo dos Santos Almeida

Infantry Aspirant of Guarda Nacional Republicana

Figure 20 - Letter of Introduction in English 2/7

INFORMED CONSENT PROTOCOL

This protocol is established between Diogo dos Santos Almeida, a student at the Military Academy carrying out research on the subject of "*Freelance Terrorism, methods of prevention and combat: A comparative study between Portugal, Poland and France*", and the participant_____, through the interview method.

The researcher and scientific supervisor undertake to:

a) Conduct the research in accordance with the quality parameters recommended by the scientific community of the specialty;
b) Discuss and negotiate other case-specific aspects relating to the confidentiality of information, if requested by the participant;
c) Prevent any disclosure of information about participants outside the research team without the prior consent of all those involved;
d) Deliver a descriptive summary of the results to the participants by email;
e) Keep participants informed of the work being carried out, particularly with regard to analysing the data, whenever they so request;
f) Provide participants in the process with any clarifications requested during the course of the research;
g) Comply with the Code of Ethics of the American Psychological Association (APA 7th edition) when carrying out the research;
h) Delete all audio recordings after the research and the public defence of the thesis.

Figure 21 - Letter of Introduction in English 3/7

Participants undertake to:

a) Provide information about their experience in the case under study and their professional experience;
b) Be interviewed at a time agreed between the researcher and the participant;
c) Authorize the audio recording of the interview at the request of the researcher;
d) Decide to mention or omit their participation in the project in professional contexts where they consider it appropriate to do so;
e) Allow the results of the study to be published, with their identity omitted, namely in the following situations:
I. Master's thesis to be submitted to the Military Academy;
II. Communications at scientific-professional congresses;
III. Scientific publications in specialized journals and/or books.

Signatures:

_____
(Participant)

_____
(Researcher)

Place and Date:

_____

Figure 22 - Letter of Introduction in English 4/7

IDENTIFICATION OF THE INTERVIEWEE

Name:	**Time (Start/End):**
U/E/O:	**Date:**
Function/Rank:	**Place:**

INTERVIEW

Your answers are fundamental to achieving the objectives of the research, so we ask that they be as complete as possible. Your answers will be used solely and exclusively as an object of study for the research, which is why you are asked to authorize the recording and subsequent analysis and transcription of your answers, in the knowledge, however, that they will be deleted as provided for in the protocol. If it is your intention, the answers will be made available to you together with the final work as soon as it has been approved.

Question 1 – What role does your institution play in combating terrorism in Poland?

Question 2 – How does your institution define and characterize Freelance Terrorism?

Question 3 – What are the main profiles of Freelance Terrorists? And which ones have been identified in Poland?

Question 4 – Do you consider this form of terrorism is on the rise in Poland? Why?

Question 5 – What are your institution's main strategies for preventing Freelance Terrorism?

Question 6 – What are your institution's main strategies for combating Freelance Terrorism?

Question 7 – How is coordination between the different Polish institutions in the fight against this threat?

Question 8 – Is there an effective sharing of information with other European organisations? What is the role of this sharing?

Figure 23 - Letter of Introduction in English 5/7

Question 9 – How would you assess cooperation between Poland and other European countries in the fight against terrorism? And in particular with Portugal, how would you assess this collaboration and what are the specific protocols? In particular with the GNR (National Republican Guard of Portugal)?

Question 10 – What challenges arise in international collaboration in the fight against Freelance Terrorism? And in particular with Portugal?

Question 11 – Is the current legislation sufficient/adequate to deal with this threat, or would reforms be necessary?

Question 12 – What are the main challenges faced in the fight against Freelance Terrorism in Poland?

Question 13 – What is the role of the individual agent in the fight against Freelance Terrorism? Do you think that the individual action of an agent within the security systems is relevant to the fight against Freelance Terrorism?

Question 14 – How do you assess the importance of HUMINT (Human Intelligence) in detecting and preventing Freelance Terrorist threats? What other intelligence gathering methods does your institution use and what are the challenges?

Question 15 – How can artificial intelligence be used to support Freelance Counter-Terrorism strategies and what are the challenges? Are there any concrete applications already implemented in Poland?

Question 16 – What is your opinion on the French Vigipirate Plan as a national strategy to prevent and combat terrorism? Do you think that the measures implemented by France through this plan are effective in the fight against terrorism, particularly Freelance Terrorism?

Figure 24 - Letter of Introduction in English 6/7

Question 17 – Do you think that other countries, notably Portugal, would benefit from implementing a plan similar to the Vigipirate Plan? What would you think would be the advantages and challenges of such an initiative in a different context?

Question 18 – What recommendations would you make to improve the prevention of and fight against Freelance Terrorism in Poland?

Question 19 – Can you identify any other points that you think should be addressed?

Thank you for your cooperation.

Figure 25 - Letter of Introduction in English 7/7

APPENDIX J – INTERVIEWEES' CHARACTERISATION, CODING MATRICES AND CORRELATION ANALYSIS

Table 16 - Characterisation of the interviewees to whom interview guide type A

ID	Rank	Entity	Role	Mode	Date	Interview Guide
E1	Lieutenant Colonel	UCAT-SSI	GNR Permanente Representative at UCAT	In Person	25february25	A
E2	-	SIS-SIRP	SIRP Cabinet	E-Mail	17march25	A
E3	Lieutenant Colonel	DI-GNR	Acting Director of DI	E-Mail	27march25	A

Table 17 - Characterisation of the interviewees to whom interview guide type C

ID	Rank	Entity	Role	Mode	Date	Interview Guide
E4	Sargent	FORMOZA	\	In Person	25april25	C
E5	Commander	GROM	\	In Person	25april25	C

Table 18 - Coded Register Units and Contextual Segments from Interview Guide A (Portugal)

Q	Interviewee	Context Unit	Coded Register Unit
1	E1	"The UCAT's main role in counter-terrorism in Portugal is to ensure cooperation and information sharing among the entities that comprise it, including police forces, intelligence services, the Maritime Police, and the Public Prosecutor's Office."	1.1 – Interinstitutional coordination and information sharing
		"UCAT includes a permanent technical team composed of six representatives, one from each operational entity, who ensure uninterrupted functioning."	1.2 – Permanent technical structure for continuous coordination
	E2	"The SIS operates within the national intelligence system and is responsible for producing information relevant to internal security, particularly for anticipating and preventing threats such as terrorism."	1.3 – Strategic intelligence production for threat anticipation

		“It conducts intelligence gathering and analysis in close cooperation with national and international entities to detect and mitigate emerging risks.”	1.4 – Intelligence-based detection and international cooperation
	E3	“The GNR ensures internal security and the protection of citizens' rights and freedoms. As a front-line force, it must be prepared to respond to all types of threats, including terrorism.”	1.5 – Constitutional and operational responsibility for internal security
		“Its role includes preventing and combating terrorism through vigilance, public order, and readiness, in line with its general mandate.”	1.6 – Preventive and tactical readiness against terrorism
2	E1	“We do not define this type of terrorism in a detailed or specific way. UCAT aims to combat terrorism broadly, regardless of whether it is perpetrated by lone actors or organised groups.”	2.0 – No specific institutional definition; broad and transversal approach
	E2	“Although the term 'freelance terrorism' is not officially used by SIS, it is equivalent to 'individual terrorism'. It refers to isolated actors, often influenced by extremist ideologies online.”	2.1 – Isolated individuals influenced by extremist content (digital or ideological)
	E3	“Freelance terrorism involves actors operating independently, without hierarchical structure or organisational affiliation, often driven by ideology or personal motives.”	2.1 – Isolated individuals influenced by extremist content (digital or ideological)
		“The phenomenon is difficult to monitor and is likely to increase, given the quality and accessibility of extremist propaganda, often AI-enhanced and available in European Portuguese.”	2.2 – Online propaganda and technological amplification increase difficulty of detection
3	E1	“This question is closely related to the previous one, so I have nothing further to add.”	3.0 – No contribution provided
	E2	“Profiles have proven heterogeneous, although traits such as social marginalisation, psychological instability, and digital radicalisation are common.”	3.1 – Psychosocial vulnerability and exposure to digital radicalisation
		“In Portugal, the threat level remains low, but there are ongoing cases under monitoring suggesting self-radicalisation.”	3.2 – Ongoing monitoring of self-radicalised individuals in Portugal
	E3	“The terrorist threat is increasingly diffuse, and without organisational links, it is harder to establish a profile in freelance terrorism.”	3.3 – Difficulty in establishing a profile due to absence of affiliation
		“There is a trend among younger individuals, especially minors aged 12–17, exposed to extremist content online in gaming chats and closed platforms.”	3.1 – Psychosocial vulnerability and exposure to digital radicalisation
		“Radicalisation can occur rapidly through access to online content, without need for sophisticated planning or access to restricted materials.”	3.4 – Rapid radicalisation enabled by accessible digital propaganda
		“Fortunately, there has been no recent terrorist activity in Portugal allowing the identification of specific freelance terrorist profiles.”	3.2 – Ongoing monitoring of self-radicalised individuals in Portugal

4	E1	“We cannot make any assertion as to whether this form of terrorism is increasing or not. Such a conclusion would be bold and unfounded.”	4.0 – No inference possible due to lack of sufficient data
	E2	“Although the national context remains relatively stable, the global spread of extremist ideologies—particularly online—requires constant vigilance.”	4.1 – Stability at national level with increased digital radicalisation risk
		“Risk increases as individuals find in the internet a conducive environment for self-indoctrination.”	4.2 – Self-indoctrination facilitated by online environments
	E3	“In recent years there have been no terrorist attacks allowing us to assess whether this form is increasing or decreasing in Portugal.”	4.0 – No inference possible due to lack of sufficient data
		“At the European level, particularly in central Europe, jihadist-related attacks and arrests have increased, according to the TE-SAT reports.”	4.3 – European-level increase in jihadist threats (TE-SAT reference)
5	E1	“The main strategies are not those of UCAT specifically, but rather of the National Strategy to Combat Terrorism (ENCT), approved in 2023. This is the central instrument guiding prevention and response.”	5.1 – National Counter-Terrorism Strategy (ENCT) as overarching framework
	E2	“SIS focuses on monitoring radicalisation phenomena, analysing social and digital dynamics, and cooperating with national and international entities.”	5.2 – Monitoring radicalisation and interinstitutional cooperation
		“We also promote societal and institutional resilience by raising awareness of emerging risks.”	5.3 – Risk awareness and resilience-building initiatives
	E3	“All terrorist threats are continuously assessed as part of risk evaluation operations conducted by the Intelligence Directorate.”	5.4 – Continuous risk assessment in operational planning
		“We invest in training at all levels to raise awareness, particularly among officers in community policing and crime prevention sections.”	5.5 – Institutional training focused on terrorism complexity
		“We participate in national and international forums to update our situational awareness and learn best practices.”	5.6 – Participation in forums for updated awareness and best practices
		“OSINT capabilities are used to detect extremist content or signs of radicalisation online, with the information shared within UCAT.”	5.7 – Open-Source intelligence for online radicalisation detection
		“External communication includes awareness campaigns targeting young people, warning them about terrorist use of digital platforms for recruitment.”	5.3 – Risk awareness and resilience-building initiatives
6	E1	“I respond in the same way as to question 5.”	6.1 – National Counter-Terrorism Strategy (ENCT) as overarching framework
	E2	“Combat is carried out through early detection of radicalisation indicators, cooperation with operational and judicial entities, and the production of intelligence that anticipates risky behaviours.”	6.2 – Intelligence-led early detection and interagency cooperation
	E3	“Combat strategies are outlined in the Coordination Plan for the Operational Command and Control of Security Forces, a classified document.”	6.3 – Tactical-police response based on classified coordination plan

7	E1	“Coordination is ensured through regular weekly operational meetings and secure communication systems for data exchange among UCAT entities. Extraordinary meetings may also be convened.”	7.1 – Permanent coordination via weekly meetings and secure communication
	E2	“Interinstitutional coordination occurs through structures such as the Security Coordination Office (GCS) and through bilateral links between SIS and police or judicial entities.”	7.2 – Coordination via formal structures and bilateral operational channels
	E3	“The Coordination Plan outlines how different entities articulate their response to terrorist situations, but it is classified and restricted to authorised personnel only.”	7.3 – Coordination protocols defined in classified operational plan
8	E1	“Yes, information is shared both at peer level — between UCAT/SSI and similar structures in Europe — and bilaterally through the entities that comprise UCAT, such as the PJ or SIS.”	8.1 – Existence of structured international information sharing
		“The types of information are diverse and specifying them would not make much sense here.”	8.2 – Types of information not specified
	E2	“Yes. SIS participates in platforms such as the Berne Club and the EU Counter Terrorism Group (CTG), regularly sharing threat intelligence, suspect profiles, and modus operandi.”	8.1 – Existence of structured international information sharing
	E3	“Yes. Through Europol and other platforms, we share information relevant to police work and monitor the TE-SAT report on terrorism trends and current threats.”	8.1 – Existence of structured international information sharing
		“Cooperation involves police, government, and academic bodies; the threat is transnational and requires ongoing information sharing.”	8.3 – Exchange of threat intelligence, profiles, and modus operandi (shared by E2 and E3)
9	E1	“Collaboration with France is not particularly different from that with other European countries. Protocols are mostly defined by the legal frameworks of each country.”	9.1 – Positive cooperation based on shared legal and institutional structures
	E2	“Collaboration with European partners is positive, with established bilateral and multilateral channels. In the case of France, information exchange benefits from their experience.”	9.1 – Positive cooperation based on shared legal and institutional structures
	E3	“Collaboration is evaluated positively. Secure information channels are used, and there’s a shared goal of preventing attacks and prosecuting offenders.”	9.1 – Positive cooperation based on shared legal and institutional structures
		“Macro-level protocols include the EU Security Union Strategy and the EU Counter-Terrorism Strategy to align member states’ efforts.”	9.2 – Formalised EU strategic cooperation frameworks
10	E1	“There are no significant differences in how we cooperate with France compared to other European partners. Cooperation is positive and fluid, though it can always be optimised.”	10.1 – Cooperation with France does not differ from EU norm
			10.2 – Functional cooperation with room for optimisation
	E2		10.1 – Cooperation with France does not differ from EU norm

		“Key challenges include legislative harmonisation, data protection restrictions, and institutional differences. Cooperation with France is constructive but requires adaptation.”	10.3 – Legal and institutional asymmetries as obstacles
	E3	“Before combating freelance terrorism, it is necessary to prevent it. Prevention relies heavily on information sharing. In this area, I don’t see significant challenges, as secure channels are increasingly used.”	10.1 – Cooperation with France does not differ from EU norm
			10.2 – Functional cooperation with room for optimisation
11	E1	“The current legislation is sufficient. We have laws on internal security, counter-terrorism, criminal investigation, and a national strategy.”	11.1 – Existing legislation is generally sufficient
		“However, the regulatory decree governing UCAT (Decree No. 2/2016) must be revised to reflect institutional and legal developments, such as the dissolution of SEF.”	11.2 – Institutional/legal evolution requires revision of specific legislative instruments
	E2	“Legislation has evolved with the threat, but legal instruments must be constantly reviewed given the rapidly changing modus operandi of terrorist actors.”	11.2 – Institutional/legal evolution requires revision of specific legislative instruments
	E3	“Overall, legislation is sufficient for conventional threats.”	11.1 – Existing legislation is generally sufficient
		“Biggest challenge lies in coordination between actors, which requires training and simulation exercises.”	11.3 – Operational coordination remains a practical challenge
		“We are slowly adapting to online radicalisation; the EU Digital Services Act has not yet been transposed.”	11.4 – Need for legal transposition regarding digital radicalisation
12	E1	“The main challenge is the early detection of behaviours or risk indicators, ideally before an incident occurs or at least to mitigate its impact.”	12.1 – Early detection of behavioural indicators to prevent or minimise attacks
		“Many past incidents in Europe involved individuals already known to the authorities; detection failure is often post-facto.”	12.2 – Operational blind spots despite prior institutional awareness
	E2	“Main challenges include early detection of radicalisation, identification of digital threats, and balancing security with privacy rights.”	12.1 – Early detection of behavioural indicators to prevent or minimise attacks
		“Emerging threats arise in digital contexts, which are difficult to anticipate.”	12.2 – Operational blind spots despite prior institutional awareness
		“There is a constant tension between security measures and protection of fundamental rights, particularly privacy.”	12.3 – Legal-ethical tension between surveillance and data protection
	E3	“This threat is hard to detect due to its isolated, unaffiliated nature. Individuals act alone and access content on the dark web or anonymous platforms.”	12.1 – Early detection of behavioural indicators to prevent or minimise attacks
		“Radicalisation happens rapidly and anonymously through gaming platforms and closed chat groups, making monitoring difficult.”	12.4 – Use of hidden or encrypted platforms for radicalisation
		“Terrorist financing often involves cryptocurrency, complicating traceability of funds and transactions.”	12.5 – Use of cryptocurrencies for terrorist financing
		“Individuals can find online how to commit attacks without needing sophisticated equipment.”	12.6 – Accessibility of online terrorist resources without organisational support

13	E1	"The role of the individual agent, such as a police officer, is essential—especially in terms of being trained and alert to detect signs of risk behaviour."	13.1 – Individual vigilance and training are key to early detection
	E2	"The agent's role is crucial in observing behaviour, reporting internally, and responding in a timely manner to risk indicators. Training and awareness are fundamental."	13.1 – Individual vigilance and training are key to early detection
	E3	"Yes, absolutely. Whether on duty or off-duty, every military officer is a sensor—an antenna—for identifying relevant information. Their observations may be valuable for intelligence."	13.2 – Officers as continuous human sensors contributing to intelligence flow
		"We include this in training across all categories and encourage sharing observations that may support interagency intelligence collaboration."	13.1 – Individual vigilance and training are key to early detection
14	E1	"I would prefer not to comment on this question."	14.0 – No comment provided
	E2	"HUMINT plays a central role in identifying early signals and sensitive contexts. It is complemented by SIGINT, OSINT, and institutional cooperation, facing legal and technical challenges."	14.1 – HUMINT as a core component in early detection
			14.2 – Intelligence integration and adaptive constraints
	E3	"HUMINT is increasingly essential to detect terrorist actors early, especially when OSINT cannot access the required information."	14.2 – Intelligence integration and adaptive constraints
		"We rely heavily on OSINT tools to retrieve data on individuals, based on their digital footprint."	14.3 – OSINT tools as operational intelligence resource
		"Challenges of OSINT include data volume and verifying the reliability of the information gathered."	14.4 – OSINT limitations: data overload and reliability issues
15	E1	"Artificial intelligence is relevant today. One potential application is in optimising data analysis, including criminal and other types of intelligence information. Many tools are available on the market."	15.1 – AI as a complementary tool for optimised data and criminal intelligence analysis
	E2	"AI can enhance large-scale data analysis, behaviour pattern detection, and risk anticipation in digital environments. There are pilot projects underway, still in exploratory stages."	15.1 – AI as a complementary tool for optimised data and criminal intelligence analysis
			15.2 – Ethical and legal challenges of AI implementation
	E3	"AI offers advanced tools for multi-source data analysis, pattern and trend detection, and facial recognition, particularly through image/video alarm systems."	15.1 – AI as a complementary tool for optimised data and criminal intelligence analysis
		"Challenges include understanding what data is stored in large databases and aligning AI use with legal frameworks like Data Protection."	15.2 – Ethical and legal challenges of AI implementation
16	E1	"I will not comment on this question or the next one."	16.0 – No comment provided
	E2	"The Vigipirate Plan is a robust and multifaceted strategy that mobilises resources, ensures institutional coordination, and involves civil society. It has shown effectiveness."	16.1 – Vigipirate as a comprehensive and effective French strategy

	E3	"The plan provides scalable responses based on a national alert system. For example, in 2015, military patrols were deployed in high-traffic and touristic areas. It had a deterrent effect."	16.1 – Vigipirate as a comprehensive and effective French strategy
		"Its effectiveness depends on intersectoral coordination and societal engagement. Measuring effectiveness is complex due to the unpredictable and diffuse nature of the threat."	16.2 – Efficacy is context-dependent and difficult to quantify
17	E1	"No comment."	17.0 – No comment provided
	E2	"Portugal has effective mechanisms of prevention and response, but a more integrated national plan could improve institutional communication and operational coordination."	17.1 – A national plan could improve coordination and institutional communication
	E3	"We must consider the different security environments in France and Portugal. While threat levels are high, Portuguese society is not as sensitised to terrorism, which complicates implementing restrictive measures."	17.2 – Lack of public awareness and absence of domestic attacks hinder acceptability
		"Even so, UCAT is a crucial national body for prevention, particularly due to its role in coordination and information sharing."	17.1 – A national plan could improve coordination and institutional communication
18	E1	"The legislation is adequate but must be updated to reflect the current operational reality—particularly the decree discussed in Q11."	18.1 – Legislative adequacy with need for targeted updates
		"We must not neglect the human factor—continuous training and awareness among agents is essential for early detection."	18.2 – Continuous training and awareness for frontline personnel
	E2	"Improve digital literacy, strengthen interagency coordination, promote specialised training, and enhance monitoring of digital ideological content."	18.2 – Continuous training and awareness for frontline personnel
			18.3 – Digital surveillance and institutional coordination as priority domains
	E3	"We have a solid legal framework and operational flexibility. The terrorist threat level rose after the 07/11/2023 Hamas attack, prompting strengthened security measures."	18.1 – Legislative adequacy with need for targeted updates
			18.4 – Dynamic adaptation of measures based on evolving threat levels
19	E1	"Nothing specific, except to say it is positive that someone is addressing these topics, even in academic research. This field tends to be discreet and underdiscussed, which is natural but not always desirable."	19.0 – No relevant additional information
	E2	"It is important to value the role of civil society and local communities as early detection agents. Proximity-based strategies built on trust and cooperation are essential."	19.1 – Civil society and community trust as pillars of early detection
	E3	"No further comments."	19.0 – No additional input

Source: Own elaboration using MAXQDA software

Table 19 - Coded Register Units and Contextual Segments from Interview Guide C (Poland)

Q	Interviewee	Context Unit	Coded Register Unit
1	E4	"Our unit is a tactical police force. We intervene when a threat is identified, supporting high-risk arrests and securing strategic locations. Operations follow intelligence-led directives."	1.1 – Tactical intervention under operational command from intelligence services
	E5	"We support Poland's counter-terrorism system through prevention, intelligence, special operations, and strategic readiness. There have been no official attacks, but preparedness remains essential."	1.1 – Tactical intervention under operational command from intelligence services
			1.2 – Strategic readiness and preventive posture in a non-attack environment
2	E4	"Freelance terrorism involves individuals or small groups acting independently, not under formal terrorist command. They're often radicalised online and unpredictable."	2.1 – Independent action by individuals or small groups without organisational affiliation
			2.2 – Online radicalisation as a core feature
	E5	"It refers to violent acts by individuals or small groups operating independently of recognised terrorist organisations. These actors are usually self-radicalised online and lack structured support, which makes detection difficult."	2.1 – Independent action by individuals or small groups without organisational affiliation
			2.2 – Online radicalisation as a core feature
			2.3 – Absence of structured support networks increases detection difficulty
3	E4	"We haven't had active attacks, but we monitor isolated individuals with access to extremist content online. Some have shown signs of radicalisation, but no attacks followed."	3.1 – Monitored profiles include isolated individuals accessing online extremist content
			3.3 – Signs of radicalisation are monitored even without active attacks
	E5	"Profiles usually involve socially isolated, ideologically driven individuals. In Poland, we've intercepted people posing as refugees on the eastern border, fitting risk profiles."	3.1 – Monitored profiles include isolated individuals accessing online extremist content
			3.2 – Individuals disguised as refugees used to destabilise Europe
			3.4 – Profiles marked by ideological motivation over criminal background
			3.5 – Border securitisation as a mechanism to intercept radicalised infiltrators
4	E4	"Although no attacks have occurred, the risk is present due to global dynamics. The spread of online radical content and foreign ideological influence is concerning."	4.1 – Freelance terrorism is perceived as an emerging concern due to global radicalisation trends
	E5	"Yes, the threat is increasing. Digital exposure to extremist content and ease of access to materials for low-tech attacks raise the risk. Early prevention has helped."	4.1 – Freelance terrorism is perceived as an emerging concern due to global radicalisation trends
			4.2 – Digital proliferation and low-tech means heighten threat levels despite absence of attacks

5	E4	"Our role in prevention is indirect. We contribute through readiness and rapid deployment. Intelligence and monitoring fall under specialised agencies."	5.1 – Indirect preventive role through operational readiness and support to intelligence efforts
	E5	"We focus on monitoring, community engagement, cooperation with other agencies, and intelligence-led policing. Education and outreach are also emphasised, although not directly executed by us."	5.1 – Indirect preventive role through operational readiness and support to intelligence efforts
			5.2 – Emphasis on community engagement, early intervention, and inter-agency coordination
6	E4	"We intervene when a threat is confirmed. Our duties include tactical action, suspect apprehension, and site control, always under intelligence directives."	6.1 – Tactical deployment and direct intervention under intelligence-led command
	E5	"Even without actual attacks, we ensure combat readiness through tactical training, HUMINT, surveillance tech, and regular simulation exercises."	6.1 – Tactical deployment and direct intervention under intelligence-led command
			6.2 – Simulation, HUMINT, and technology to anticipate and neutralise freelance
7	E4	"Coordination is strong, particularly through joint training and operational planning. Tactical forces depend on clear communication from central command."	7.1 – Coordination through joint training, planning, and command-chain communication
	E5	"Coordination is robust and improving. Intelligence, police, military, and emergency services collaborate via joint task forces and threat monitoring hubs."	7.1 – Coordination through joint training, planning, and command-chain communication
			7.2 – Centralised intelligence-sharing hubs and task-force structures
8	E4	"Yes. We don't manage data exchange directly, but intelligence shared through Europol and similar platforms informs our threat assessments and operational posture."	8.1 – Intelligence sharing through Europol informs national tactical and threat decisions
	E5	"Yes. Collaboration with Europol, Frontex, and EU partners is crucial to identify cross-border threats and tactics. It supports strategic planning, especially given Poland's geographical relevance."	8.1 – Intelligence sharing through Europol informs national tactical and threat decisions
			8.2 – Intelligence exchange supports strategic planning in a geopolitically exposed country
9	E4	"Cooperation is generally good. I don't interact directly with foreign agencies but sometimes join multinational exercises. I'm not aware of direct links with the GNR."	9.1 – Multinational cooperation occurs mainly through exercises; no known links to GNR
	E5	"Cooperation across the EU is constructive. We haven't had direct cooperation with Portugal or the GNR, but their role in EU-wide platforms is recognised. Knowledge-sharing could be deepened."	9.1 – Multinational cooperation occurs mainly through exercises; no known links to GNR
			9.2 – Potential to deepen cooperation with GNR in training and joint operations
10	E4	"Differences in procedures, language, and legal frameworks can delay information sharing. Although coordination is improving, real-time collaboration remains difficult."	10.1 – Linguistic, procedural, and legal differences hinder real-time international cooperation

	E5	"Legal barriers, data protection regulations, and diverging national priorities can obstruct cooperation. With Portugal, more structured frameworks and streamlined exchange are needed."	10.1 – Linguistic, procedural, and legal differences hinder real-time international cooperation
			10.2 – Collaboration with Portugal is underdeveloped; liaison structures and information channels should be enhanced
11	E4	"The legal framework is solid, especially since no attacks have occurred. But more agile judicial tools and improved digital surveillance would help address evolving threats."	11.1 – Existing legal framework is sufficient but lacks agility in digital surveillance and judicial procedures
	E5	"The law is adequate, but must evolve. Cyber-radicalisation, encrypted communications and preventive detention require legislative updates. Reforms must also protect civil liberties."	11.1 – Existing legal framework is sufficient but lacks agility in digital surveillance and judicial procedures
			11.2 – Legal reforms must balance evolving security needs with fundamental rights
12	E4	"The main challenge is early detection. Individuals acting alone are hard to identify without strong intelligence. Public awareness and reporting are also limited."	12.1 – Early detection of lone actors is hindered by lack of intelligence and limited public vigilance
	E5	"Freelance terrorists don't operate in visible networks. Private radicalisation and lack of criminal history make them hard to trace. The absence of attacks limits societal engagement."	12.1 – Early detection of lone actors is hindered by lack of intelligence and limited public vigilance
			12.2 – Low threat visibility reduces political and societal investment in prevention
13	E4	"Each operator must remain alert and strictly follow procedures. Personal discipline and readiness are essential, especially in fast-response environments."	13.1 – Discipline, vigilance and procedural rigour at individual level support rapid-response readiness
	E5	"Absolutely. Agents are crucial in spotting warning signs, engaging with communities, and reacting swiftly. Their training and instinct often make the difference in stopping lone actors."	13.1 – Discipline, vigilance and procedural rigour at individual level support rapid-response readiness
			13.2 – Field agents' intuition and community contact are key to early detection of lone actors
14	E4	"HUMINT is crucial at the community level. We also use technical surveillance and cyber intelligence. Privacy and legal constraints are significant challenges."	14.1 – HUMINT remains vital, especially at the community level
			14.2 – Cyber intelligence and surveillance face legal/privacy barriers
	E5	"HUMINT is essential in vulnerable environments. We also apply SIGINT, OSINT, and behavioural analytics. The main challenge is ensuring civil liberties in low-threat contexts."	14.1 – HUMINT remains vital, especially at the community level
			14.2 – Cyber intelligence and surveillance face legal/privacy barriers
			14.3 – Preventive intelligence in low-threat countries raises proportionality and liberty concerns
15	E4	"AI can detect radical patterns and enhance threat analysis. Poland is exploring these capabilities, but there are no large-scale implementations I am aware of."	15.1 – AI holds potential for detecting radical content and enhancing threat assessment
			15.2 – Poland is in exploratory phase; no major deployments yet
	E5		15.1 – AI holds potential for detecting radical content and enhancing threat assessment

		"AI is already used in pilot projects: social media scanning, pattern recognition, predictive models. Challenges include privacy, bias, and human validation."	15.2 – Poland is in exploratory phase; no major deployments yet
			15.3 – Algorithmic bias, privacy concerns, and need for human oversight are key challenges
16	E4	"It's a good example of layered alert levels and visible deterrence. A national plan like Vigipirate supports both prevention and coordinated response."	16.1 – Vigipirate valued as a deterrence tool and multi-level coordination model
	E5	"The plan is theoretically strong and adaptable. It promotes public awareness and communicates risk levels effectively. Its principles could inform Polish policy, though our society differs."	16.1 – Vigipirate valued as a deterrence tool and multi-level coordination model
			16.2 – Vigipirate features could be adapted, but national sociopolitical context must be considered
17	E4	"Yes, but each country must adapt it. A visible security presence and public communication can help prevent freelance attacks and boost civilian confidence."	17.1 – Vigipirate-type plans could be beneficial if adapted to national context
			17.2 – Visible deterrence and public reassurance are key advantages
	E5	"Such a model could improve readiness and raise awareness, but must be adapted to threat level and avoid overreaction in low-risk settings. Cultural and societal sensitivity is essential."	17.1 – Vigipirate-type plans could be beneficial if adapted to national context
			17.3 – Implementation must be proportional and culturally adapted to national risk perception
18	E4	"Strengthen early detection, train personnel to recognise radicalisation signs, enhance inter-agency communication, and conduct regular drills to prepare tactical responses."	18.1 – Improve early detection, inter-unit coordination and response simulation
			18.2 – Expand training to recognise behavioural indicators
	E5	"Boost online monitoring, support deradicalisation programmes, train frontline agents, increase international cooperation, and promote social resilience through media literacy and counter-narratives."	18.1 – Improve early detection, inter-unit coordination and response simulation
			18.2 – Expand training to recognise behavioural indicators
			18.3 – Invest in deradicalisation, digital monitoring and public resilience
19	E4	"We should invest more in officer mental health, encourage public engagement through education, and improve international coordination on digital threats."	19.1 – Promote officer well-being and mental health
			19.2 – Foster public engagement through education
			19.3 – Enhance international cooperation in digital surveillance
	E5	"We must not ignore foreign disinformation and hybrid threats. Strengthening police-community trust is key. But above all, the priority is prevention over post-incident response."	19.4 – Address hybrid threats and foreign disinformation
			19.5 – Prioritise prevention over reaction
			19.6 – Strengthen trust between police and local communities

Source: Own elaboration using MAXQDA software

Table 20 - Quantitative analysis of the frequency of segments per question in Interview Guide A

Question	Category	SubCategory	Coded Register Unit	Interviewee			Enumeration Units	Results (%)
				1	2	3		
Interview Guide A								
1	Institutional Structure	Responsibilities and Actions	1.1	X			1	33%
			1.2	X			1	33%
			1.3		X		1	33%
			1.4		X		1	33%
			1.5			X	1	33%
			1.6			X	1	33%
2	Concept	Typology and Framework	2.0	X			1	33%
			2.1		X	X	2	67%
			2.2			X	1	33%
3	Phenomenon Characterisation	Profiles and Behaviours	3.0	X			1	33%
			3.1		X	X	2	67%
			3.2		X	X	2	67%
			3.3			X	1	33%
			3.4			X	1	33%
4			4.0	X		X	2	67%
			4.1		X		1	33%
			4.2		X		1	33%
			4.3			X	1	33%
5	Prevention Mechanisms	National Strategies	5.1	X			1	33%
			5.2		X		1	33%
			5.3		X	X	2	67%
			5.4			X	1	33%
			5.5			X	1	33%
			5.6			X	1	33%
			5.7			X	1	33%
6	Combat Mechanisms		6.1	X			1	33%
			6.2		X		1	33%

			6.3			X	1	33%
7	Interinstitutionality	Internal Cooperation	7.1	X			1	33%
			7.2		X		1	33%
			7.3			X	1	33%
8	International Cooperation	Information Sharing and Protocols	8.1	X	X	X	3	100%
			8.2	X			1	33%
			8.3			X	1	33%
9			9.1	X	X	X	3	100%
			9.2			X	1	33%
10			10.1	X	X	X	3	100%
			10.2	X		X	2	67%
			10.3		X		1	33%
11	Legal Framework	Need for Reforms	11.1	X		X	2	67%
			11.2	X	X		2	67%
			11.3			X	1	33%
			11.4			X	1	33%
12	Operational Challenges	Practical Limitations	12.1	X	X	X	3	100%
			12.2	X	X		2	67%
			12.3		X		1	33%
			12.4			X	1	33%
			12.5			X	1	33%
			12.6			X	1	33%
13	Individual Capacities	Responsibility and Initiative	13.1	X	X	X	3	100%
			13.2			X	1	33%
14			14.0	X			1	33%
			14.1		X		1	33%
			14.2		X	X	2	67%
			14.3			X	1	33%
			14.4			X	1	33%

15	Artificial Intelligence	Methods and Limitations	15.1	**X**	**X**	**X**	3	100%
			15.2		**X**	**X**	2	67%
16	Comparative Models	Good Practice Transfers	16.0	**X**			1	33%
			16.1		**X**	**X**	2	67%
			16.2			**X**	1	33%
17			17.0	**X**			1	33%
			17.1		**X**	**X**	2	67%
			17.2			**X**	1	33%
18	Suggestions	Measures and Enhancements	18.1	**X**		**X**	2	67%
			18.2	**X**	**X**		2	67%
			18.3		**X**		1	33%
			18.4			**X**	1	33%
19	Open Insights	Additional Perspectives	19.0	**X**		**X**	2	67%
			19.1		**X**		1	33%

Table 21 - Quantitative analysis of the frequency of segments per question in Interview Guide C

Question	Category	SubCategory	Coded Register Unit	Interviewee		Enumeration Units	Results (%)
				4	5		
Interview Guide C							
1	Institutional Structure	Responsibilities and Actions	1.1	**X**	**X**	2	100%
			1.2		**X**	1	50%
2	Concept	Typology and Framework	2.1	**X**	**X**	2	100%
			2.2	**X**	**X**	2	100%
			2.3		**X**	1	50%
3	Phenomenon Characterisation	Profiles and Behaviours	3.1	**X**	**X**	2	100%
			3.2		**X**	1	50%
			3.3	**X**		1	50%
			3.4		**X**	1	50%
			3.5		**X**	1	50%
4			4.1	**X**	**X**	2	100%
			4.2		**X**	1	50%
5	Prevention Mechanisms	National Strategies	5.1	**X**	**X**	2	100%
			5.2		**X**	1	50%
6	Combat Mechanisms		6.1	**X**	**X**	2	100%
			6.2		**X**	1	50%
7	Interinstitutionality	Internal Cooperation	7.1	**X**	**X**	2	100%
			7.2		**X**	1	50%
8	International Cooperation	Information Sharing and Protocols	8.1	**X**	**X**	2	100%
			8.2		**X**	1	50%
9			9.1	**X**	**X**	2	100%
			9.2		**X**	1	50%
10			10.1	**X**	**X**	2	100%
			10.2		**X**	1	50%

11	Legal Framework	Need for Reforms	11.1	**X**	**X**	2	100%
			11.2		**X**	1	50%
12	Operational Challenges	Practical Limitations	12.1	**X**	**X**	2	100%
			12.2		**X**	1	50%
13	Individual Capacities	Responsibility and Initiative	13.1	**X**	**X**	2	100%
			13.2		**X**	1	50%
14			14.1	**X**	**X**	2	100%
			14.2	**X**	**X**	2	100%
			14.3		**X**	1	50%
15	Artificial Intelligence	Methods and Limitations	15.1	**X**	**X**	2	100%
			15.2	**X**	**X**	2	100%
			15.3		**X**	1	50%
16	Comparative Models	Good Practice Transfers	16.1	**X**	**X**	2	100%
			16.2		**X**	1	50%
17			17.1	**X**	**X**	2	100%
			17.2	**X**	**X**	2	100%
			17.3		**X**	1	50%
18	Suggestions	Measures and Enhancements	18.1	**X**	**X**	2	100%
			18.2	**X**	**X**	2	100%
			18.3		**X**	1	50%
19	Open Insights	Additional Perspectives	19.1	**X**		1	50%
			19.2	**X**		1	50%
			19.3	**X**		1	50%
			19.4		**X**	1	50%
			19.5		**X**	1	50%
			19.6		**X**	1	50%

Table 22 - Correlation by word similarity between interviewees

Correlation Between Interviewees		Pearson Correlation Coefficient
File A	File B	
E1	E2	0,175
E4	E5	0,161
E1	E3	0,130
E2	E5	0,121
E2	E3	0,115
E3	E5	0,108
E1	E5	0,095
E2	E4	0,082
E1	E4	0,058
E3	E4	0,036

Source: Own elaboration using MAXQDA software

In order to further analyse the qualitative data collected, a Pearson correlation was applied using the MAXQDA software, focusing on identifying lexical patterns shared by the interviewees. This approach made it possible to examine the existence of linear relationships between the frequency of occurrence of certain words or expressions, especially those that recurred throughout the interviews, making it possible to identify relevant discursive convergences in the context of the phenomenon under study. The added value of this technique lies in its ability to quantify linguistic similarities between participants, making it possible to highlight points of consensus, terminological alignment or even trends in collective discourse. The process consisted of lexical coding of the speeches, extracting relative frequencies and subsequently analysing the correlation between these linguistic variables, contributing to a more robust and integrated reading of the qualitative data.

The low lexical similarity coefficients observed among the interviewees (between 0,036 and 0,175) indicate a significant dispersion in the vocabularies used to describe the phenomenon of Freelance Terrorism. This lexical heterogeneity, far from being a limitation, is consistent with the non-normative and multifaceted nature of the object of study itself. As the phenomenon is constantly changing and has different implications for institutional and national contexts, this diversity is highly relevant. In a comparative study such as this one, this result reinforces precisely the relevance of the approach, by demonstrating there are no consensus understandings and practices regarding the definition, prevention and fight against terrorism, either at national or international level.