SELINUS UNIVERSITY
OF SCIENCES AND LITERATURE

Terrorism and Security in the European Union (2015 - 2025)

By Kyriakos Vlachokyriakos

A THESIS

Presented to the Department of International Relations
program at Selinus University

Faculty of Arts & Humanities
in fulfillment of the requirements
for the degree of Doctor of Philosophy
in International Relations

2025

Table of Contents

Chapter 1: Introduction

1.1 Background of the Study

Over the past decade, the European Union has faced a security environment that has become ever more intricate and unpredictable, and while terrorism is by no means a new spectre on its soil, nothing quite prepared citizens and policymakers for the wave of attacks that began in 2015 because these events combined shocking brutality with a level of coordination and adaptability that challenged conventional assumptions about how violence could be planned and carried out. The horrific scenes in Paris and the later bombings in Brussels laid bare not only gaps in border checks and delays in intelligence sharing but also deeper questions about how individuals who were born and raised within European communities could come to embrace extremist ideologies by way of online echo chambers and personal grievances. At the same time, Europe was contending with larger geopolitical tremors caused by conflicts in the Middle East and North Africa which drove migration surges and sparked intense debates about solidarity and security, debates that often pitted the urgent need to keep people safe against the equally vital commitment to protect human dignity and uphold the rule of law. Because these attacks involved figures who exploited the freedom of movement within the Schengen Area and who used encrypted apps and social media platforms as readily as anyone might use a messaging service, the EU found itself compelled to rethink its approach in a way that went beyond simply tightening controls, moving instead toward a more cohesive framework that fused law enforcement cooperation with community engagement, revised legal instruments, and cutting edge technology for threat analysis. Still, the expansion of data gathering tools and new databases came with serious concerns about privacy and oversight because the same measures that could help identify planning for violence could also erode the personal freedoms that define open societies. And yet, despite those legitimate worries, many officials agreed that no single country could face the changing face of terrorism alone and that genuine resilience would arise only through true collaboration involving shared training exercises, joint analysis centres and real time alerts that could help prevent small sparks of radicalization from exploding into large scale tragedies (Czaplicki, 2021).

Meanwhile, as the nature of the threat evolved from hierarchical networks to loosely connected lone actors whose methods were less predictable and more difficult to track, the EU's response had to become equally dynamic, combining legal reforms with educational campaigns, digital surveillance with deradicalization programs, and national initiatives with Europe wide task forces that could pool resources and expertise. And while new artificial

intelligence tools and advanced analytics promised faster detection of suspicious patterns and better allocation of security resources, they also prompted lively discussion about accountability and fairness because algorithms can inherit the biases of their creators and because broad data sweeps run the risk of ensnaring those who pose no real danger. Therefore, the challenge has always been to ensure that every new capability is matched by robust checks and balances so that the Union can protect its people without sacrificing the liberties that make Europe a place worth defending. Understanding how all these moving parts, operational imperatives, technological potential, legal safeguards and political, willhave interacted over the period from 2015 to 2025 is essential if we hope to learn the right lessons and craft strategies that both shield citizens from harm and preserve the open and democratic values at the heart of the European project. This study sets out to explore that complex and evolving journey, tracing the decisions and debates that have shaped the EU's counterterrorism landscape, and aiming to reveal not just what has been achieved but also where tensions remain and where fresh thinking may be needed(Bures, 2016).

1.2 Statement of the Problem

Over the past decade the European Union has made considerable efforts to build a stronger and more unified response to the threat of terrorism, yet it continues to grapple with the fundamental challenge of balancing the urgent demand for effective security measures with its deep commitment to democratic values and the protection of individual freedoms. And while instruments such as the Passenger Name Record directive and upgrades to the Schengen Information System were introduced with the aim of improving cross-border information sharing and speeding up the identification of potential threats that same technological advance has raised fresh questions about whether these tools have truly created a coherent and resilient security network across all twenty-seven member states. Because terrorism itself has transformed over these years from centrally planned attacks in which large cell structures were identified and dismantled into a more dispersed phenomenon shaped by self-radicalized individuals operating in isolation or in small groups the Union's traditional reliance on centralized databases and formal police cooperation has at times struggled to keep pace with this new reality. And even though emerging technologies such as artificial intelligence driven analytics offer the promise of quicker detection of suspicious patterns, they also bring troubling concerns about privacy and bias and the risk that citizens may lose faith in security services if appropriate legal and ethical safeguards are not put in place (Martinico & Dembinski, 2021).

Meanwhile the political and legal landscape in which these security measures must operate remains uneven because member states differ widely in their legal traditions in their institutional capabilities and in their willingness to cede elements of national sovereignty to EU-level coordination. And as a result, directives that look sound on paper are implemented with varying levels of enthusiasm and resource allocation which creates gaps in the collective defence that can be exploited by those determined to do harm. And because these gaps often exist at the borders between cooperation and hesitation, they undermine the very idea of a Security Union that relies on mutual trust and shared responsibility rather than each country standing alone. At the same time the spread of digital platforms has transformed the battlefield of ideology because social media networks encrypted messaging apps and online forums now serve as both fertile ground for radicalization and a constant headache for law enforcement agencies that must contend with conflicting platform policies and patchy agreements over data access. And while governments push for broader powers to request user information in real time technology companies and civil rights advocates warn of the dangers of unchecked surveillance and of allowing security concerns to crowd out fundamental rights.On top of these domestic challenges the EU has found itself caught up in broader geopolitical upheavals because conflicts in neighbouring regions have driven waves of migration that in turn have been seized upon by extremist narratives and by political movements that conflate human mobility with insecurity and therefore every step toward tighter border management or faster asylum processing risks becoming a flashpoint in the wider debate over solidarity and safety. And as European citizens demand both stronger protection and greater transparency governments are forced to walk a tightrope between demonstrating decisive action and preserving the trust that comes from open democratic governance. Therefore, the core problem that this study seeks to examine is how the European Union can forge a counterterrorism strategy that is at once operationally robust technologically adaptive and yet also firmly grounded in the rule of law in shared political will and in respect for human rights and individual dignity. And by exploring the evolution of the Union’s policy instruments the dynamics of intergovernmental cooperation the impact of emerging technologies and the voice of civil society this research aims to illuminate the persistent gaps and unresolved tensions that continue to shape Europe’s response to terrorism and to suggest pathways for a security model in which safety and liberty truly reinforce each other (Mitsilegas, 2018).

1.3 Aim of the Study

The primary aim of this study is to delve into the ways in which the European Union has grappled with the shifting landscape of terrorism between 2015 and 2025 and to assess whether its policy responses have managed to keep pace with increasingly fluid and unpredictable threats while still honouring the democratic values, human rights and legal safeguards that lie at the heart of the Union. In particular, the research will trace the evolution of key instruments such as directives on passenger data and enhanced data sharing arrangements alongside the rollout of systems for real time alerts and emerging technologies that promise to detect warning signs of violence before they materialize, because understanding both the technical and political layers of these initiatives is essential to gauging their true impact. Because the nature of terrorism has transformed markedly during this period, from large scale networks with clear command structures to lone actors and loosely connected cells who exploit social media and encrypted messaging, the study also aims to evaluate how effectively the EU's traditionally centralized frameworks for cooperation and intelligence exchange have adapted to these new modes of radicalization and violence. At the same time, it will consider whether the shift toward more proactive and data driven approaches has been accompanied by sufficient safeguards against excessive intrusion into personal privacy or against the unfair targeting of minority communities, since the very tools that can save lives can also become instruments of mistrust if wielded without care. Moreover, the research intends to shed light on the dynamic between EU level recommendations and the varied ways in which national capitals have translated those recommendations into practice, because member states continue to differ in their legal traditions, their institutional capacities and even their political appetite for pooling sovereignty in the name of common security. By comparing implementation across several countries, the study will highlight examples of successful cooperation and identify persistent roadblocks that undermine collective resilience when individual interests outpace shared concerns (Machado & Liesching, 2019).

In addition, the study will engage with the voices of civil society groups, front line practitioners and affected communities so that policy analysis is grounded in lived experience and public sentiment as well as in official reports and legal texts. This emphasis on diverse perspectives recognizes that counterterrorism policy does not exist in isolation but is shaped by societal debates about migration, social justice and the very meaning of security in open societies. Finally, the research will explore the unintended ripple effects that can accompany powerful surveillance and predictive analytics tools when clear boundaries and oversight

mechanisms are lacking, and it will examine how questions of transparency, oversight and democratic accountability have been raised or neglected throughout the policy making process. By combining document analysis, expert interviews and illustrative case studies the study aims to provide a holistic picture of the EU's counterterrorism journey, revealing not only where coherence and effectiveness have been achieved but also where fragmentation and ethical tension continue to challenge the European project. Ultimately the goal is to offer evidence based insights and practical recommendations that can guide future strategies so that policy makers at both EU and national level can learn from past successes and missteps and forge a security framework that is not only operationally robust and technologically savvy but that also remains firmly rooted in the principles of democracy, solidarity and human dignity which define the European Union (Howorth &Gheciu, 2018).

1.4 Research Questions

This study is guided by two central research questions that together frame a comprehensive exploration of how the European Union has navigated the shifting terrain of terrorism between 2015 and 2025 while striving to uphold its democratic principles and the rule of law. The first question asks how the EU's counterterrorism framework has evolved in response to a transformation from large hierarchical networks to more fluid and often self-radicalized individuals and loosely connected cells and whether the introduction of measures such as passenger data directives, enhanced information sharing agreements and emerging real time threat detection systems has fostered genuine cooperation among member states even as it has respected individual privacy and bolstered public trust. By examining this question, the study will trace the journey of policy from conception to implementation and will compare the legislative intent with the operational realities on the ground while seeking to understand the political and institutional choices that shape when and how these instruments are deployed (Machado & Liesching, 2019).

The second question turns to the inherent tensions and trade-offs that arise when powerful surveillance tools, algorithmic analytics and predictive data driven prevention strategies intersect with the EU's foundational commitments to solidarity, transparency and human rights and it asks to what extent the deployment of artificial intelligence, big data analytics and proactive policing technologies has altered both the capabilities and the boundaries of counterterrorism practice and whether these advances have been matched by effective oversight mechanisms, meaningful public dialogue and safeguards against unintended consequences such as biased profiling or a chilling effect on free speech. By addressing this

question, the study will explore how civil society organisations, media narratives and judicial bodies have influenced the acceptance or rejection of new security measures, and how the balance between operational necessity and legal or ethical constraint has been negotiated across different national and institutional contexts. Together these two questions provide a clear yet flexible framework that allows this research to illuminate where resilience and solidarity have grown stronger, where fragmentation or ethical tension persists, and where fresh thinking may be needed to harmonize the twin imperatives of safety and liberty. Through a methodology that combines document analysis, expert interviews and illustrative case studies this study aims to uncover practical and evidence-based insights that can guide future policy development and help craft a counterterrorism model that remains true to the values that define the European Union(Shepherd, 2024).

1.5 Significance of the Study

This study is important because it arrives at a time when the European Union is still absorbing the lessons of some of the most devastating terrorist attacks in its history and is simultaneously wrestling with the challenge of keeping its citizens safe while preserving the freedoms and rights that lie at the heart of the Union's identity, and while many analyses have focused on individual elements of counterterrorism policy or on specific technological innovations, this research brings together legal reforms, political dynamics, technological advances and social implications so that we can see how each of these pieces interacts with the others in practice. Because terrorism has shifted from highly organised networks with clear hierarchies to individuals and small groups who radicalise themselves online and plan attacks with minimal infrastructure, it is essential to trace how high level agreements in Brussels translate into everyday practice in local police stations, border posts and community centres, and to understand whether those practices truly foster a sense of collective security rather than simply imposing new layers of surveillance. At the same time this study recognises that genuine resilience depends on more than cutting edge tools and directives, since the quality of cooperation across twenty-seven diverse member states varies according to legal traditions, resource levels and political will, and it explores how these differences can either strengthen the Security Union or create gaps that malicious actors may exploit. Moreover this research contributes to a broader conversation about the balance between security and liberty in open societies because it highlights how every push for more robust data gathering, analytics and real time alerts can raise legitimate concerns about privacy, algorithmic bias and transparency, and because it shows that tackling these concerns requires

clear safeguards, independent oversight bodies and meaningful engagement with civil society organisations and rights advocates who bring vital perspectives that might otherwise be overlooked. By bringing together the voices of front-line practitioners, community leaders, legal experts and policy makers the study ensures that its conclusions rest on a foundation of lived experience as well as strategic vision, and it demonstrates that effective counterterrorism must build and maintain public trust if it is to succeed. Ultimately the value of this work lies in its ambition to offer practical and evidence based recommendations that respect the European Union's core principles of democracy, solidarity and human dignity while also equipping governments with the tools and approaches they need to respond swiftly and effectively to evolving threats, so that future strategies can not only prevent violence but also strengthen the bonds of trust and cooperation that make open societies both safe and free (Martinico & Dembinski, 2021).

1.6 Scope and Limitations of the Study

This research focuses on the European Union's counterterrorism efforts between 2015 and 2025 and examines how legal instruments, operational frameworks, technological tools and social dynamics came together to address a changing threat that shifted from tightly controlled networks to individuals who radicalize themselves online, and while the study gives particular attention to directives on passenger data, shared information systems and emerging real time threat detection methods, it also considers how these measures played out in practice across member states whose legal traditions and institutional capacities vary considerably. Because these ten years encompass some of the most significant policy reforms in the Union's history as well as the rapid rise of digital innovations such as artificial intelligence and big data analytics, the analysis is necessarily wide ranging, but it remains anchored in the core question of how effective, coherent and rights respecting these responses have been when set against the real world complexities of implementation. At the same time this study acknowledges its own limits because access to classified intelligence and internal law enforcement procedures is restricted, and so it relies primarily on publicly available legal texts, policy evaluations, expert interviews and illustrative case studies to build a detailed picture of how measures were designed, adopted and adapted on the ground in police stations community centres border checkpoints and crisis coordination centres. And although the research touches on the role of emerging technologies, it approaches them from a policy and governance perspective rather than as a deep technical audit of algorithms or software systems, because the main aim is to assess their societal and legal implications rather than

their engineering details. Moreover this study recognises that national variations in political will, resource allocation and public opinion can create gaps in collective resilience, and it therefore examines a representative mix of member states to highlight both best practices and persistent obstacles, while not attempting a full comparative survey of all twenty seven countries because such an undertaking would require resources and data beyond the scope of a single thesis. And while the research seeks to integrate the voices of civil society practitioners and affected communities alongside policymakers and security experts, it remains limited by the availability and willingness of certain stakeholders to engage, which means that some perspectives may be more visible than others.Finally, this study is bounded by its time frame which ends in 2025, and so it cannot account for developments or lessons learned beyond that point, but it does aim to draw forward looking conclusions that will remain relevant as new challenges and opportunities arise. By clarifying these boundaries, the research strives to deliver a focused yet comprehensive evaluation of how the European Union has worked to protect its citizens without losing sight of the freedoms and values that define it(Hartmann, 2022).

1.7 Organisation of the Thesis

This thesis unfolds in a way that mirrors the progression of its central questions and allows the reader to move seamlessly from context to conclusion, beginning with Chapter One which introduces the background and rationale of the research, outlines the aim and objectives, presents the core research questions and explains the study's scope and significance so that the reader understands why and how the investigation has been framed. Chapter Two then offers a comprehensive literature review in which key academic debates, policy frameworks and theoretical perspectives on terrorism and security governance in the European Union are brought together and assessed side by side to reveal both well-trodden ground and gaps that this research aims to address. Following this, Chapter Three describes the methodology by explaining how documents, policy texts, interviews and case studies have been selected and analysed, and by reflecting on the advantages and constraints of a qualitative, policy-oriented approach so that the reader can grasp not only the methods themselves but also the reasoning behind their use. Chapter Four presents the empirical findings by detailing how specific EU directives, information-sharing mechanisms and emerging technologies were introduced and adapted in practice, and by illustrating through examples in several member states where cooperation succeeded or where challenges persisted. Chapter Five then engages in a critical discussion of these findings by weaving together insights from the literature review,

methodology and empirical data to assess whether the Union's counterterrorism framework has achieved coherence, effectiveness and respect for fundamental rights, and to consider the trade-offs and unintended consequences that have surfaced along the way. Finally, Chapter Six draws the study to a close by summarising the main contributions, offering evidence-based recommendations for future EU and national policy development, and pointing to areas where further research could deepen our understanding as the European Union continues to adapt its approach to the evolving threat of terrorism.

Chapter 2: Literature Review

Conceptual Foundations of Terrorism and Security

The conceptual edifice upon which European counter-terrorism policy has been erected rests upon two interlocking constructs, terrorism and security, whose meaning is anything but settled, since each term has been continuously re-elaborated in response to shifting historical circumstances, evolving political agendas and widening scholarly perspectives; consequently, every serious enquiry into the Union's counter-terrorism trajectory must begin by tracing how these notions have been defined, contested and ultimately operationalised within the EU's dense legal and institutional architecture. Although the Framework Decision 2002/475/JHA offers a functional definition that treats terrorism as the commission of serious crimes intended to intimidate a population, coerce governments or destabilise social structures, the very need for such an instrument betrays the absence of an uncontested conceptual core: Member States continue, often quite legitimately, given their differing constitutional traditions, to interpret and apply this definition in divergent ways, a reality that complicates both legislative harmonisation and the day-to-day business of police and judicial cooperation (Schmid, 2011; Bures, 2016). At the theoretical level, early research sought explanatory power in the individual psyche, positing that certain personal traits or pathologies could account for extremist violence; yet later waves of scholarship, disillusioned with reductionist models, re-centred the analysis on socio-economic grievances, perceived political exclusion and identity-based cleavages, thereby depicting radicalisation as a process nurtured by structural inequities and catalysed by global communications networks that magnify outrage and confer a seductive sense of belonging (Crenshaw, 1981; Gurr, 2006). This more expansive lens has proved indispensable for understanding Europe's recent experience with home-grown violent extremism, because many perpetrators were neither clandestine infiltrators nor disciplined cadres but rather European citizens who, feeling alienated in their own societies, found in online echo chambers a narrative that reframed personal frustration as collective struggle.

In parallel, the very idea of security has undergone a remarkable metamorphosis, for the classical image of the state warding off external armies now sits uneasily beside a reality in which non-state actors, porous digital spaces and global flows of people, goods and data generate threats that defy territorial boundaries and hierarchical command structures; thus, contemporary security debates revolve around the question of how to protect not only borders and critical infrastructure but also individual rights, social cohesion and democratic

legitimacy (Buzan, Wæver & de Wilde, 1998; Howorth &Gheciu, 2018). The EU's distinctive embrace of "human security" underscores that tension, because Brussels is expected to foster freedom of movement, economic prosperity and fundamental rights even while coordinating decisive action against terrorism; the Union must, therefore, reconcile its normative commitment to liberty with the political imperative of safety, a balancing act rendered still more delicate by the distribution of competences between supranational bodies and sovereign capitals (Martinico & Dembinski, 2021). In that milieu, securitisation theory, pioneered by the Copenhagen School, offers a valuable interpretive tool: it posits that an issue becomes a matter of "security" when influential actors successfully cast it as an existential threat, thereby legitimising extraordinary measures that would be unacceptable under normal conditions (Buzan et al., 1998; Balzacq, 2011). The EU's post-2015 policy repertoire, which ranges from the Passenger Name Record Directive to the repeated upgrades of the Schengen Information System, vividly illustrates how terrorism has been framed as a danger so acute that it warrants expanded surveillance powers, accelerated information exchange and novel forms of predictive policing (Czaplicki, 2021).

Yet securitisation is a double-edged sword, since the same rhetoric that galvanises, cooperation can erode civil liberties and foster the stigmatisation of minority communities; critics therefore insist that emergency measures remain subject to rigorous proportionality tests, transparent oversight and sunset clauses that prevent the normalisation of exceptional powers (Mitsilegas, 2018; Machado & Liesching, 2019). These normative safeguards have become all the more salient as artificial-intelligence systems and big-data analytics promise to identify suspicious patterns with unprecedented speed, while simultaneously raising spectres of algorithmic bias, opaque decision-making and mission creep that could undermine public trust in both national authorities and EU institutions (Shepherd, 2024). Indeed, because counter-terrorism increasingly relies on anticipating rather than reacting to violence, the Union's security paradigm has shifted towards risk management: that is, the systematic identification, ranking and mitigation of potential harms in a world where zero risk is unattainable and absolute prevention illusory (Beck, 2006). This risk-based logic permeates border control, aviation security and critical-infrastructure protection, urging policymakers to allocate resources where statistical models suggest the greatest marginal benefit, even though such models may rest on contestable assumptions and incomplete data.

Trust therefore emerges as both lubricant and litmus test of the entire machinery: without mutual confidence among Member States, sensitive intelligence will not flow swiftly enough to pre-empt attacks, yet without the confidence of citizens, especially those who feel

disproportionately scrutinised, the legitimacy of security practices will erode, perhaps fuelling the very radicalisation they are meant to prevent (Hartmann, 2022). Scholars of governance consequently emphasise the importance of inclusive policy processes that engage local authorities, civil-society organisations and frontline communities, because those actors possess contextual insights that rarely appear in threat matrices yet prove crucial for early intervention and social resilience (Vidino et al., 2017). Moreover, empirical studies have shown that preventive programmes grounded in education, employment support and community dialogue often yield more sustainable results than purely repressive strategies, pointing to the need for a holistic approach in which law enforcement, social services and cultural initiatives reinforce rather than undermine one another.

All these theoretical strands, contested definitions, structural explanations, securitisation dynamics, risk governance and participatory legitimacy, converge in the European project, whose legal order embeds strong human-rights guarantees even as its political mandate demands effective action against terrorism. The Charter of Fundamental Rights, the jurisprudence of the Court of Justice of the European Union and the jurisprudence of the European Court of Human Rights delineate outer limits that counter-terrorism measures must respect, thereby ensuring that policy innovation remains anchored in values of dignity, proportionality and non-discrimination; nevertheless, the very pluralism of the EU means that every legislative or operational advance is the product of negotiation among actors with diverging histories, capacities and normative preferences, a fact that explains why gaps in implementation persist and why constant monitoring, evaluation and adjustment are indispensable (Machado & Liesching, 2019; Martinico & Dembinski, 2021). Ultimately, then, the conceptual foundations of terrorism and security within the Union are best understood not as a fixed blueprint but as an evolving conversation, one conducted in parliamentary chambers, courtrooms, ministerial councils and online forums, about how an open society can defend itself without betraying the principles that render it worth defending in the first place.

Against that backdrop, the present thesis proceeds on the assumption that conceptual clarity is a prerequisite for empirical rigor: only by recognising how definitions shape data collection, how securitising moves influence resource allocation, and how risk metrics interact with social trust can researchers accurately assess whether EU counter-terrorism policy between 2015 and 2025 has become more coherent, more effective and more rights-respecting. By weaving together insights from political science, sociology, legal studies and critical security theory, the literature reviewed here underscores the analytical pay-off of a multidisciplinary

perspective, while simultaneously reminding us that the struggle over meaning is itself a site of political power. As terrorism mutates in form, embracing lone actors, encrypted communication and transnational logistical hubs, so too must our conceptual tools evolve, lest we fall into the trap of fighting yesterday's battles with yesterday's paradigms; conversely, if policymakers allow fear to dictate the terms of debate, then the circle of securitisation may tighten until it chokes the liberal freedoms whose defence ostensibly justified the measures in the first instance. The challenge, therefore, is to cultivate a reflexive security culture that prizes empirical evidence, welcomes critical scrutiny and remains steadfastly committed to the Union's founding credo of "unity in diversity," because only such a culture can simultaneously reduce vulnerability to violence and nurture the democratic vitality upon which enduring security ultimately depends.

In conclusion, the conceptual category of terrorism acquires intelligibility only in relation to broader socio-political contexts, while the concept of security derives its normative bite from the imperative to safeguard both collective order and individual autonomy; therefore, European counter-terrorism can be judged successful only to the extent that it embeds robust safeguards against abuse, fosters trust across multiple levels of governance and addresses the root causes of radicalisation rather than merely its violent symptoms. This literature review, by mapping the contested terrain on which those concepts are forged and re-forged, sets the stage for the empirical chapters that follow, which will examine how the EU's sprawling policy apparatus has grappled in practice with the doctrinal tensions, operational dilemmas and ethical quandaries outlined here, in order to determine whether the period 2015–2025 represents a decisive stride towards a Security Union that is as respectful of liberty as it is resilient against terror.

Evolution of Terrorist Threats in the EU

The trajectory of terrorist threats across the European Union between the mid-2010s and the midpoint of the 2020s can only be understood as a fluid continuum in which successive waves of violence, ideological mutation and technological adaptation unfolded in mutually reinforcing cycles, and, crucially, as a story in which every apparent lull in spectacular attacks merely concealed the gestation of new modalities of extremism that would later erupt in altered form, thus demanding a perpetual recalibration of analytical frameworks and policy instruments alike. Whereas the preceding century had already exposed Europe to separatist, ethno-nationalist and ideologically polarised violence, think, for instance, of ETA's long insurgency in Spain or the Provisional IRA's campaign in Northern Ireland, the first decade

and a half of the twenty-first century ushered in a qualitatively different threat environment, since the collapse of territorial safe havens in Afghanistan and, later, the chaos in Iraq and Syria enabled transnational jihadist networks to embed themselves symbiotically within Europe's open societies, thereby converting global grievances into hyper-localised acts of terror whose choreography exploited the very freedoms they sought to destroy (Bakker, 2015; Coolsaet, 2016).

The carnage that unfolded in Paris in January and again in November 2015, followed by the bombings in Brussels in March 2016, served as an unmistakable inflection point, because those meticulously coordinated attacks, carried out by cells whose members moved with unsettling ease across Schengen's internal borders, combined military-grade weaponry, encrypted communications and a chilling readiness for self-annihilation, thereby shattering the lingering illusion that terrorism could be contained at the Union's external frontiers and revealing instead an endogenous menace rooted in alienation, social fragmentation and digital echo chambers within the Member States themselves (Vidino et al., 2017). In the aftermath of those atrocities, security practitioners and scholars alike were forced to acknowledge that the classic focus on dismantling hierarchical organisations, so effective against earlier generations of militant groups, had been outpaced by a new model of networked extremism whose operational nodes were often siblings, childhood friends or petty criminals radicalised online, and whose logistical backbone comprised small-scale arms trafficking, peer-to-peer financing and opportunistic exploitation of returning foreign fighters (EUROPOL, 2016).

Yet even as the Islamic State gradually lost its proto-state in the Levant under sustained military pressure from 2017 onward, the threat did not dissipate but rather reconfigured itself in more atomised and therefore more elusive forms; indeed, deprived of its territorial sanctuary, IS issued global communiqués encouraging sympathisers to conduct improvised attacks wherever they resided, an exhortation that dramatically lowered the organisational threshold for violence and thus ushered in the era of the so-called lone actor, although, as numerous case studies demonstrate, "lone" seldom means socially or ideologically isolated, since most perpetrators continued to draw validation, tactical advice and ideological reinforcement from dense virtual communities linked by encrypted platforms and algorithmically curated propaganda streams (Neumann, 2017; Reed et al., 2019). Consequently, the operational repertoire shifted from spectacular multi-site assaults, Paris, Brussels, Istanbul, towards lower-cost but still devastating methods such as the vehicular massacre on Nice's Promenade des Anglais in July 2016, the knife and van attack at London Bridge in June 2017 and the combined firearm and machete assault on Vienna's city centre in

November 2020, events that collectively underscored how rudimentary instruments can inflict strategic shock when paired with instantaneous media amplification and a public already sensitised to insecurity.

Simultaneously, the ideological spectrum of violent extremism widened appreciably, because while jihadist narratives retained potency, the late 2010s also witnessed the mainstreaming of far-right conspiracies, accelerationist manifestos and white-supremacist tropes on the very same digital platforms that had incubated jihadist radicalisation a decade earlier; this ideological diversification rendered obsolete any counterterrorism doctrine rooted in a single adversarial archetype and instead compelled agencies to adopt threat-agnostic methodologies capable of spanning anti-Semitic assaults such as the Halle synagogue shooting in 2019, anti-Muslim plots exemplified by the thwarted mosque bombing in France, and hybrid anti-government conspiracies that gestated in pandemic-era online communities (EUROPOL, 2022). The COVID-19 crisis, moreover, acted as an accelerant in its own right, insofar as prolonged lockdowns, economic precarity and institutional mistrust created psychological and socio-political breeding grounds for extremist recruitment, while the surge in online activity provided both an expanded audience for disinformation and an unpoliced arena for operational planning; thus, even though large-scale attacks became statistically rarer during the strictest phases of confinement, intelligence services warned that kinetic dormancy did not equate to ideological retreat but often signified strategic patience (Junge et al., 2021).

Parallel to these ideological and tactical shifts, a quieter yet no less consequential transformation was unfolding in the cyber domain, where terrorist actors, sometimes overlapping with state-sponsored proxies, experimented with attacks designed less to cause immediate casualties than to erode public confidence in critical services, manipulate information ecosystems, or exploit latent vulnerabilities in energy grids and transport networks; and while fully fledged “cyber-terrorism” in the sense of catastrophic digital sabotage has remained largely hypothetical, the convergence of ransomware techniques, deepfake technologies and disinformation campaigns has convinced many analysts that future iterations of terrorism may well manifest as blended operations whose digital prongs soften societal targets before physical violence occurs (Brundage et al., 2020). Recognising this trajectory, the EU sought preventative leverage through instruments such as Regulation (EU) 2021/784 on the swift removal of online terrorist content, yet the implementation of such measures revealed disparities in technical capacity, legal culture and civil-liberties safeguards across Member States, thereby fuelling debates over proportionality, transparency and the risk of utilising automated filters that might unintentionally censor legitimate speech

(Machado & Liesching, 2019; Martinico & Dembinski, 2021).

The geographical diffusion of attacks added yet another layer of complexity, because, whereas earlier spectaculars tended to target cosmopolitan capitals, Paris, Madrid, London, recent incidents have increasingly struck provincial towns, regional transport hubs and places of worship far from media epicentres, a pattern that simultaneously taxes local police forces, heightens the perceived ubiquity of danger and fractures the conceptual distinction between "hard" and "soft" targets; indeed, as perpetrators pivot towards opportunistic assaults on venues ranging from Christmas markets to hospital car parks, the protective perimeter expands into virtually every domain of daily life, obliging policymakers to enlist municipal authorities, school administrators and grassroots organisations as front-line partners in prevention (Reed et al., 2019). Such decentralisation inevitably challenges intelligence architecture predicated on centralised databases, because effective early warning now depends as much on community reporting and social-service referrals as on SIGINT and biometric alerts, and it compels the reconceptualization of resilience not as a static fortress-like state but as an adaptive capacity dispersed throughout society.

Notwithstanding the proliferation of technological solutions, artificial-intelligence flagging, biometric border checks, behavioural analytics, the literature converges on the insight that upstream social interventions remain indispensable, since radicalisation incubates in micro-contexts shaped by familial rupture, peer dynamics, local grievances and identity quests; thus, investments in education, vocational programmes, intercultural dialogue and restorative justice have been shown to reduce both susceptibility to extremist narratives and recidivism among returned foreign fighters, even though such initiatives rarely receive the sustained political capital afforded to high-visibility security hardware (Bouhana & Wikström, 2011). Moreover, empirical studies demonstrate that heavy-handed or discriminatory policing can backfire by reinforcing the very perceptions of injustice that extremist recruiters weaponize, suggesting that counterterrorism must be mediated through a proportionality lens that safeguards fundamental rights while still enabling decisive disruption of imminent threats.

Consequently, the evolution of terrorist threats in the European Union should be viewed less as a linear progression from one dominant typology to another than as a kaleidoscopic process in which multiple threat vectors, jihadist, far-right, single-issue, cyber-enabled, coexist, overlap and intermittently cross-fertilise, creating a strategic environment characterised by continual surprise, ideological hybridity and operational bricolage. Within such an environment, the Union's comparative advantage lies in its ability to orchestrate multi-level governance, harness the analytic power of agencies like Europol, and uphold a

normative order grounded in the Charter of Fundamental Rights; yet that same multi-layered structure also generates friction points, legal diversity, data-protection constraints, resource asymmetries, that adversaries may exploit unless inter-institutional trust and technical interoperability are strengthened (Bures, 2016; Mitsilegas, 2018).Ultimately, then, the decade under review reveals a dual imperative: on the one hand, to refine detection and disruption capabilities in step with an adversary whose tactics continually mutate across ideological and technological domains, and, on the other, to cultivate social cohesion, civic trust and rights-based governance without which any purely coercive counter-terrorism architecture is destined to erode its own legitimacy. Only by sustaining this delicate equilibrium, between vigilance and restraint, innovation and accountability, can the European Union hope to shield its diverse communities from episodic bursts of extremist violence while preserving the democratic ethos that renders those communities resilient, pluralistic and worth defending.

EU Counter-Terrorism Instruments and Frameworks

The dense lattice of post-2015 European Union counter-terrorism law has been spun progressively, each strand reflecting lessons drawn from successive waves of violence as well as from jurisprudential and technological change, so that by the middle of the 2020s the Union possesses an apparatus at once wider in substantive reach, deeper in operational integration and more tightly hemmed in by fundamental-rights guarantees than anything imagined when the first EU counter-terrorism strategy appeared two decades earlier. Because an effective legal backbone is indispensable, the principal normative anchor is Directive (EU) 2017/541, which repealed the 2002 Framework Decision and, by criminalising travel for terrorist purposes, recruitment, training, public provocation, financing and the facilitation of such conduct, ensured that prosecutors throughout the Union could pursue the full lifecycle of terrorist activity under largely convergent definitions, thereby closing loopholes that perpetrators had previously exploited whenever an act outlawed in one jurisdiction fell outside the criminal code of another (Directive (EU) 2017/541, 2017).

Yet the harmonisation of offences would have been sterile had it not been coupled with instruments designed to track the movement of persons whose intentions were concealed behind legitimate mobility rights, and for that reason Directive (EU) 2016/681 on Passenger Name Record data obliges air carriers to transmit booking files to nationally designated Passenger Information Units so that algorithmic risk engines, operating under strict data-protection and retention safeguards shaped by the Court of Justice's digital-rights jurisprudence, can compare routings, payment patterns and seat selections with profiles

extrapolated from past logistics chains, a process that allows authorities to apprehend facilitators and couriers long before traditional surveillance would have revealed their involvement (Directive (EU) 2016/681, 2016; Court of Justice of the European Union, 2022).

Because the Internet has become the principal artery through which extremist propaganda, operational manuals and ideological mentoring flow, the Union moved beyond voluntary industry "codes of conduct" and adopted Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, thereby empowering competent authorities anywhere in the EU to order hosting providers to remove flagged material within one hour while simultaneously obliging platforms to establish risk-based, transparent and rights-compliant content-moderation regimes that complement, rather than stifle, freedom of expression (Regulation (EU) 2021/784, 2021). This hard law turn in the digital domain is nested within the Security Union Strategy 2020-2025, a Commission policy roadmap that reconceives "security" as a transversal societal good and that explicitly calls for the fusion of intelligence, border management, financial investigation and cyber-resilience into a single anticipatory ecosystem (European Commission, 2020a). Barely twelve months later the Strategy's principles were operationalised by the EU Counter-Terrorism Agenda, whose four pillars, anticipate, prevent, protect and respond, promote wider use of artificial intelligence for pattern recognition, provide guidance for hardening soft targets, expand solidarity funding for victims and export EU investigative standards through capacity-building partnerships beyond the Union's frontiers (European Commission, 2020b).

Because anticipation in practice is inconceivable without interoperable data, a decisive leap occurred with the twin Regulations (EU) 2019/817 and 2019/818, which created a shared biometric-matching service, a common identity repository and a multiple-identity detector that now knit together six flagship databases, among them the Schengen Information System (SIS), the Visa Information System (VIS) and Eurodac, so that border guards, asylum officials and police investigators can, through a single interface, discover within seconds whether the individual standing before them has been recorded under another identity anywhere in Europe (Regulations (EU) 2019/817 & 2019/818, 2019). The practical dividends of that reform materialised in March 2023, when the renewed SIS entered everyday service with new alert categories for suspected foreign terrorist fighters, inquiry checks and preventive alerts, thereby granting frontline units a real-time, pan-European picture of potential threats traversing the continent (European Commission, 2023).

Raw data, however, remain inert unless rendered intelligible by analytical horsepower, which explains why Regulation (EU) 2022/991 enlarged Europol's mandate, allowing the European

Counter-Terrorism Centre to ingest very large and complex datasets, to cooperate directly with private-sector actors such as encrypted-messaging providers and financial intermediaries, and to drive controlled experimentation with lawful artificial-intelligence tools, all within a governance regime that subjects every new processing workflow to dual oversight by the European Data Protection Supervisor and a dedicated Fundamental Rights Officer (Regulation (EU) 2022/991, 2022). On the judicial flank, Regulation (EU) 2019/816 established ECRIS-TCN, a central index of convictions handed down against third-country nationals, thereby enabling prosecutors across the Union to retrieve, prior to bail or sentencing decisions, a suspect's full judicial history, including terrorism verdicts, recorded in any Member State, a facility that has proved critical when mapping the transnational itineraries of several lone-actor assailants (Regulation (EU) 2019/816, 2019).

Recognising that infrastructure itself has become both a stage and an instrument of violence, the Union adopted the Critical Entities Resilience Directive in 2022, obliging operators in sectors ranging from energy and transport to health and digital services to conduct terrorism-specific risk assessments, to implement proportionate protective measures and to notify disruptive incidents within twenty-four hours, thereby weaving counter-terrorism considerations into the broader tapestry of civil-protection and cyber-security governance (Directive (EU) 2022/2557, 2022). Looking further upstream, the Entry/Exit System, scheduled for activation in October 2025, will replace manual passport stamping with a biometric ledger that records every crossing by a non-EU traveller and matches fingerprints and facial images against EU and Interpol watch-lists, while the European Travel Information and Authorisation System, anticipated in late 2026, will vet visa-exempt visitors at the point of ticket purchase, shifting the frontier of risk assessment from the physical border to the airline check-in desk (European Commission, 2024).

An architecture of such sophistication is valuable only insofar as democratic resilience keeps pace, which is why each new dataset or investigative power is hemmed in by multilayered oversight: the European Parliament's LIBE committee examines all security-related proposals under Article 52 of the Charter of Fundamental Rights; the European Data Protection Supervisor audits Europol's algorithmic deployments; national data-protection authorities verify compliance with purpose-limitation and retention rules in the PNR and terrorist-content regimes; and the European Court of Auditors, in its 2022 special report on large-scale IT systems, criticised uneven data-quality and timeliness in Member-State contributions to SIS and related registers, prompting an EU-wide remedial action plan (European Court of Auditors, 2022).

Complementing these “hard” controls are “soft” preventive frameworks, most visibly the Radicalisation Awareness Network, which has, since 2015, disseminated community-based methodologies for disengagement, mentorship and exit programmes in prisons; likewise, Internal Security Fund and, more recently, Asylum, Migration and Integration Fund grants bankroll municipal multi-agency referral panels inspired by public-health models of early intervention, while the European External Action Service exports EU investigative and human-rights standards through technical-assistance missions in the Sahel and the Western Balkans, thereby addressing upstream the pipeline through which forged documents, weapons and extremist ideologues often reach EU soil (European Commission, 2021).

Put together, the post-2015 evolution of EU counter-terrorism instruments reveals a deliberate transition from reactive, police-centred cooperation towards an anticipatory model grounded in data fusion, algorithmic triage and proactive disruption; yet that anticipatory paradigm remains embedded in a conception of societal security which treats fundamental rights not as an inconvenient constraint but as the very condition of long-term effectiveness. Whether the synthesis endures will depend on the Union’s success in remedying persistent implementation asymmetries, sustaining public trust in an era of disinformation and technological opacity, and ensuring that every new operational capability is matched by an equal advance in transparency and accountability, thereby demonstrating, rather than merely asserting, that liberal democracy can indeed defend itself most effectively when it remains faithful to its own constitutional ethos.

Gaps, Challenges and Future Directions

Although the European Union has, since 2015, assembled an impressively dense architecture of counter-terrorism legislation, databases and coordination mechanisms, a closer reading of implementation reports, audit findings, fundamental-rights assessments and threat analyses reveals a series of structural and normative gaps that continue to inhibit the system’s full effectiveness, thereby signalling where the next wave of policy innovation and scholarly attention must concentrate.To begin with, interoperability projects have repeatedly suffered from uneven data quality and schedule slippage, a problem documented by the European Court of Auditors, which in its 2022 special report on large-scale IT systems criticised persisting deficiencies in the timeliness, completeness and accuracy of national contributions to the Schengen Information System and other shared repositories, warning that “poor data inevitably translate into poorer security outcomes” (European Court of Auditors 2022). The same report highlighted that only a handful of Member States had, by mid-2022, reached full

technical readiness for the biometric interfaces on which the common identity repository depends, while eu-LISA's 2023 annual activity report acknowledged that the Entry/Exit System and ETIAS had to be rescheduled because several capitals could not deliver new border hardware or upgrade national police back-ends on time (eu-LISA 2023). These implementation asymmetries mean that terrorists or violent extremists can still exploit the weakest national link in what aspires to be a seamless continental chain, a risk that will persist until the Commission couples financial support with firmer compliance incentives and until peer-pressure mechanisms, such as the Schengen evaluation cycle, are broadened to cover counter-terrorism data obligations as rigorously as they already cover external-border management.

A second, closely related gap concerns the governance of very large and complex datasets. Regulation (EU) 2022/991 expanded Europol's mandate to include direct ingestion of terabyte-scale dumps supplied by private companies or third-country partners, yet the European Data Protection Supervisor has repeatedly cautioned that Europol's internal tagging and deletion workflows remain too slow and too opaque, creating a residual risk that irrelevant personal data linger in agency systems long after lawful purpose has expired (EDPS 2022). The supervisory stalemate illustrates a broader tension: because machine-learning tools require vast training corpora, security authorities constantly press for longer retention, while data-protection bodies insist on strict purpose limitation; reconciling the two will require, in the medium term, investment in privacy-preserving analytics, homomorphic encryption, secure multiparty computation or federated learning, that can extract behavioural signals without exposing raw identities, as well as clearer statutory ceilings on how many years "risk-indicator" data may be kept before mandatory erasure.

Third, fundamental-rights jurisprudence has begun to reshape core instruments in ways that leave operational uncertainties. The Court of Justice's September 2022 judgment in Joined Cases C-793/19 and C-794/19 upheld the preventive value of Passenger Name Record analytics but also struck down indiscriminate bulk use for intra-EU flights, demanded stricter prior authorisation for sensitive searches and imposed tighter judicial oversight on data-retention periods; national Passenger Information Units are still adapting their algorithms and legal thresholds to those requirements, and some air carriers complain that contradictory national guidance is generating compliance costs and data-format fragmentation (CJEU 2022). Equally, the Fundamental Rights Agency's 2023 annual report warned that facial-recognition pilots at external borders "risk normalising biometric surveillance without having demonstrated necessity and proportionality", calling for ex-ante fundamental-rights impact

assessments before the full biometric Entry/Exit System goes live (FRA 2023). Until such assessments become the rule, the Union faces the double hazard of privacy litigation that undermines key tools and of a public-trust deficit that can erode voluntary cooperation by communities most affected by both terror violence and law-enforcement scrutiny.

A fourth challenge lies in the widening ideological spectrum of violent extremism. Europol's 2024 TE-SAT notes that jihadist networks remain the deadliest single category but that the fastest growth in arrests now concerns right-wing and "accelerationalist" plots, often incubated on trans-national fringe platforms that mix conspiracy theories, anti-government narratives and misogynistic subcultures (Europol 2024). Because much of the Union's prevention infrastructure, training manuals, community liaison units, prison disengagement programmes, was designed with jihadist radicalisation in mind, Member States are only gradually retro-fitting curricula to address anti-Semitic, anti-migrant and anti-state ideologies that do not fit the earlier diagnostic templates; this lag creates blind spots, particularly in smaller towns where local police lack specialised analyst capacity and where extremist content spreads through encrypted gaming chats or hybrid meme-warfare channels that are geographically dispersed and linguistically coded. Future funding calls under the Internal Security Fund should therefore ring-fence resources for ideologically neutral prevention models, and EU-wide threat-assessment tools must be recalibrated to weight social-media indicators of right-wing mobilisation as heavily as they already weight jihadist propaganda cues.

A fifth set of gaps emerges from the accelerating convergence of cyber, disinformation and kinetic threats. While full-scale cyberterrorism, e.g. blowing up a power grid solely through malware, has yet to materialise, the line between activism, criminal ransomware and ideologically motivated sabotage is blurring: the 2023 ransomware attacks on several major European hospitals, claimed by a hacker collective citing anti-vaccine conspiracy slogans, illustrated how critical-infrastructure disruption can serve terrorist messaging even when the primary motive appears financial. The 2020 Counter-Terrorism Agenda called for closer cooperation between ENISA and Europol's European Cybercrime Centre, but practical liaison is still hampered by divergent evidentiary standards, classification protocols and, above all, by the fact that many cyber incidents remain under-reported for reputational reasons (European Commission 2020b). The forthcoming Critical Entities Resilience Directive does oblige operators to file incident reports within twenty-four hours, yet enforcement capacity at national level varies widely, which implies that Brussels will need a stronger EU-CERT hub and perhaps mandatory insurance-driven disclosure rules if it expects

full visibility of hybrid attack surfaces.

Parallel to these operational frictions, political coordination itself suffers from governance fragmentation. The EU Counter-Terrorism Coordinator remains an envoy attached to the Council Secretariat, while the Commission steers legislative proposals and the High Representative leads external CT dialogues; because each body owns different instruments and budgets, strategic coherence relies on informal inter-institutional chemistry that cannot substitute for a single, empowered crisis-management chain. The 2021 Strategic Compass for Security and Defence promised to "clarify command responsibilities in the internal-security field", yet no treaty change has followed, and several capitals remain reluctant to grant the Commission direct operational leverage over intelligence-driven matters they regard as core state business. Unless this institutional puzzle is resolved, perhaps through a future Security Council configuration of ministers with a fixed presidency and an EU-level situation room, the Union risks slow collective responses whenever simultaneous attacks span multiple jurisdictions.

Moreover, many Member States still under-invest in evaluation and lessons-learned mechanisms. While aviation security benefits from regular "red team" penetration tests conducted by EU inspectors, analogous stress-tests for urban soft-targets, deradicalisation prisons or online referral mechanisms are sporadic; funding calls too often prioritise new tech over impact evaluation. To correct this, the Commission should, in its next Internal Security Fund work programme, require ex-post cost-effectiveness studies for completed CT projects and publish comparative dashboards that name laggards alongside best performers, an approach shown to drive compliance in other regulatory domains such as environmental acquis.Finally, societal trust remains both the most intangible and the most indispensable ingredient. The EDPS notes that citizens will tolerate robust data-sharing only if they believe oversight bodies can genuinely discipline abuses (EDPS 2022); simultaneously, ethnographic work from the Radicalisation Awareness Network indicates that young people who experience ethnic profiling report higher receptivity to extremist recruiters who frame law enforcement as systemic oppression (RAN 2022). Bridging that trust gap requires renewed investment in community policing, algorithmic transparency dashboards and "explainable AI" pilots that allow both judges and ordinary travellers to understand why a boarding pass was denied or an investigative flag was raised.

Chapter 3: Methodology

3.1 Research Design

The present investigation adopts an integrated qualitative design that combines structured policy analysis with elite semi structured interviewing, because such a configuration permits a balanced scrutiny of institutional frameworks and actor level perceptions while it remains fully aligned with the research questions that focus on the implementation and impact of European Union counterterrorism instruments within contrasting member states, namely France, Germany and Greece. As the European security landscape after the attacks of twenty fifteen became increasingly complex, the Union introduced a series of directives and databases that operate across legal traditions and administrative cultures, and a mono-method approach would therefore be insufficient, given that a purely doctrinal reading of legal texts illuminates statutory intentions yet neglects practice, whereas a single minded ethnographic immersion exposes lived dilemmas yet risks anecdotal generalisation, and consequently a composite design emerges as the most coherent pathway towards analytic completeness (Bures, 2016).

The research unfolds in two sequential and iteratively connected phases. In the first phase a systematic documentary analysis traces the life cycle of three flagship instruments, namely the Passenger Name Record Directive, the second generation Schengen Information System and the operational frameworks housed within Europol, starting from their promulgation at the European level, moving through national transposition, and extending to practical application, while collecting associated parliamentary debates, regulatory impact statements and oversight body reports, so that legal intent, political negotiation and administrative technique can be examined together, rather than in isolation (Machado & Liesching, 2019).

All retrieved documents are imported into a qualitative analysis platform where an a priori codebook, derived from scholarship on multilevel security governance, is complemented by inductively generated codes whenever unexpected themes surface, and this dual coding strategy ensures that theoretical guidance and empirical openness coexist productively. Subsequently the second phase introduces twenty-five elite semi structured interviews with policy makers, senior security officials, data protection regulators and civil society advocates in the three member states as well as at relevant European bodies. The interview guide is constructed after the preliminary documentary sweep, because early patterns and provisional gaps generate targeted prompts, and this sequencing follows an exploratory confirmatory

logic that strengthens validity while fostering reflexive depth. Each interview is recorded with consent, transcribed verbatim, anonymised at source, and stored in an encrypted repository that complies with institutional ethics approval and the General Data Protection Regulation. Transcripts are coded within the same analytic workspace as the documentary material, permitting matrix queries that juxtapose formal provisions with practitioner experience and thereby reveal both corroboration and divergence, which are treated as theoretically productive rather than inconvenient anomalies (Hartmann, 2022).

Comparative leverage is embedded through the deliberate selection of France, Germany and Greece, because these states exemplify divergent legal traditions, threat exposures and administrative capacities, while each participates deeply in European security arrangements. France represents a high threat civil law context that has historically embraced proactive internal security, Germany embodies a constitutional environment that foregrounds proportionality and robust judicial oversight, and Greece offers a mixed setting in which resource constraints and geopolitical pressures intersect. Treating each country first as a self contained unit and subsequently as part of a cross case synthesis maximises contextual richness while advancing theoretical replication across heterogeneous environments, and therefore the study pursues analytical generalisation rather than statistical extrapolation. Process tracing is applied to reconstruct legislative and administrative trajectories, ensuring that causal mechanisms such as policy diffusion, political bargaining and judicial constraint are not merely inferred but systematically evidenced through temporally ordered clues.

Thematic analysis of interviews proceeds through open, axial and selective coding, and intercoder reliability is assessed on a ten per cent sub sample to enhance dependability, while memo writing throughout generates an audit trail that can be externally reviewed. Triangulation is realised not simply by combining two data types, but by embedding them within a common temporal frame that spans twenty fifteen to twenty twenty-five, thereby capturing both the immediate legislative reaction to the Paris and Brussels attacks and the later technological inflection marked by artificial intelligence assisted surveillance tools.

Ethical integrity permeates the entire research architecture. All participants receive an information sheet that explains voluntary participation, the right to withdraw without consequence and the exclusive academic use of data. Personal identifiers are removed or pseudonymised, sensitive materials are stored on secure institutional servers and working files on personal devices remain anonymised, while data retention schedules follow university policy and European data protection law. In addition, a reflexive diary records positionality considerations, because the researcher acknowledges that personal background

and academic training shape interpretive choices, and this transparency supports confirmability.

Limitations are recognised so that subsequent interpretation remains proportionate. Although the multi case design enriches depth it narrows numeric breadth, and therefore the study cannot claim universal representativeness across all twenty-seven member states.

Nevertheless, the deliberate variation among the three selected cases, combined with rigorous within case analysis, seeks to demonstrate how distinct constellations of legal tradition, threat environment and administrative capacity mediate the translation of supranational directives into national practice. Reliance on elite informants may privilege official narratives; however, purposive inclusion of civil society voices and systematic juxtaposition of testimony with documentary fact mitigate this risk.

In sum, the chosen research design integrates doctrinal precision with experiential insight, embeds comparative logic and upholds ethical safeguards, and thus provides a coherent and credible foundation upon which subsequent chapters on findings, discussion and recommendations can securely build, while also contributing to broader debates on the governance of security and rights within the European Union.

3.2 Case Selection Rationale

The logic underpinning the choice of France, Germany, and Greece derives from the principle of maximum analytical contrast, given that a study which seeks to illuminate how common European Union security instruments manifest across diverse constitutional and administrative landscapes must encapsulate contexts that differ meaningfully in legal tradition, threat exposure, and governance capacity, while still remaining comparable through their shared membership obligations. As the governance of collective security in Europe unfolds through a multilevel interplay between supranational directives and domestic enactment, a tripartite selection that spans the Franco-Roman legal family, the Germanic constitutional tradition, and the comparatively mixed South-European framework allows the inquiry to observe how variation in institutional path dependence mediates both implementation performance and rights protection, and it simultaneously provides a fertile ground for theoretical replication, because findings that recur across heterogeneous settings acquire greater explanatory weight (Monar, 2020).

France constitutes the first case because it has experienced the highest concentration of lethal jihadist attacks on Union territory during the reference decade, and consequently it has served as a vanguard for expansive security legislation that seeks to reconcile emergency policing

powers with republican civil-liberty commitments. The Paris and Nice atrocities triggered the activation of extended surveillance regimes, specialised prosecution circuits, and the permanent codification of measures that were formerly justified only under temporary state-of-emergency provisions, while public support for robust counter terrorism enforcement remained comparatively high. Furthermore, French authorities played a decisive role during the drafting of the passenger name record directive and championed the acceleration of the second-generation Schengen information system, thus positioning the country as a key agenda setter in the Council. Examining France therefore allows the study to observe the upper bound of policy ambition, as well as the practical challenges that arise when anadministration pursues maximalist security reforms under tight judicial scrutiny (Bures, 2016).

Germany enriches the comparative architecture of this inquiry because its constitutional order, shaped by past experiences of intrusive state surveillance, has cultivated a sustained commitment to proportionality, judicial oversight, and strict data-protection guarantees. Although Germany has encountered terrorist incidents, its overall threat profile remains lower than that of France, while German policymakers continuously emphasise the need to align information sharing and algorithmic profiling with concrete risk assessments so that intrusive measures never exceed demonstrable security needs. The Federal Constitutional Court has repeatedly curtailed executive surveillance, intervening, for instance, in the national transposition of the Passenger Name Record instrument and in rules that govern the retention of telecommunications metadata, thereby generating a substantial jurisprudential corpus that foregrounds digital rights (Hartmann, 2022). Including Germany therefore allows the study to observe how a polity that prizes the equilibrium between security and liberty responds to supranational instruments whose operational logic often presupposes extensive data flows, while it also permits an examination of whether robust domestic privacy institutions obstruct or merely recalibrate implementation trajectories.

Greece, by contrast, offers an analytically valuable counterpoint, given that its security environment is moulded by persistent irregular migration across maritime borders, long-standing regional disputes, and intermittent domestic extremist activity, all of which must be navigated under fiscal constraints that restrict administrative capacity. Membership obligations require Greek authorities to deploy sophisticated information systems, such as the Schengen Information System, whereas limited resources compel heavy reliance on European funding arrangements and transnational operational assistance. Judicial review is conducted through a civil-law hierarchy that is less assertive than the German constitutional court,

although the national data-protection authority increasingly models its practice on European standards. Examining Greece accordingly reveals how structural limitations, and geopolitical pressures mediate the translation of supranational mandates into routine policing practice, and it illustrates the circumstances under which European solidarity mechanisms compensate for domestic capacity deficits (Machado and Liesching, 2019).

Beyond individual merits, the collective configuration of the three cases supports a most-different-systems strategy, because each country diverges along the axes of legal culture, fiscal endowment, and security threat, while they share exposure to the same European legal framework and participate in common policing forums such as Europol and FRONTEX. This configuration allows findings that converge across the trio to be attributed with greater confidence to the influence of European instruments rather than to coincidental national idiosyncrasies, given that the likelihood of alternative explanations rooted in constant country traits is reduced when cases vary widely (European Commission, 2017). Conversely, divergences that emerge despite common obligations can help isolate domestic factors that condition implementation, such as parliamentary oversight intensity or administrative professionalisation, and these divergences will feed into the comparative matrix that the findings chapter will present.

The size of the sample remains deliberately modest, because qualitative process tracing and elite interviewing demand intensive data collection and expanding the roster beyond three states would dilute analytic depth while stretching field-access feasibility. Nevertheless, the trio yields twelve potential dyadic comparisons and one triadic juxtaposition, and this geometry suffices for pattern matching and analytical generalisation, especially when the documentary corpus encompasses the full union legislation plus each national transposition statute. Furthermore, the design preserves scope for future extension, as the coding scheme and interview protocol can be transferred to additional contexts should time and resources permit.

Although the selection maximises variation, limitations are acknowledged. The absence of a Nordic civil-law case means that the sample omits a cluster with high administrative capacity and lower terrorist threat, and therefore Scandinavian insights into preventive community policing remain beyond the immediate scope. Similarly, the exclusion of a Central-Eastern member state might raise questions about post-accession adaptation, yet the choice prioritises depth over exhaustive geographical coverage, and the findings will be framed accordingly in the discussion chapter, where recommendations will specify how lessons could translate to contexts not directly studied.

In conclusion, the selection of France, Germany, and Greece accords with the dual imperative of capturing meaningful heterogeneity while sustaining methodological manageability, as it integrates contrasting legal traditions, threat intensities, and administrative capacities under a common European regulatory umbrella. This trio equips the research with the comparative leverage necessary to disentangle union level drivers from domestic mediators, thereby setting a robust empirical foundation for the subsequent data-collection procedures that the next subsection will detail, and thus ensuring that the inquiry can speak both to scholarly debates on multilevel security governance and to practitioner concerns regarding the equitable and effective implementation of counter terrorism instruments (Monar, 2020).

3.3 Data Corpus

The empirical foundation of the present inquiry rests upon a tripartite corpus that brings together European Union legislative texts, domestic legal and administrative records, and verbatim transcripts from elite interviews, given that a rounded understanding of counter terrorism governance must capture both the formal rules that articulate collective intent and the practical perspectives that shape everyday implementation, while the simultaneous consideration of these layers enables systematic triangulation that strengthens credibility (Monar, 2020).

The first stream comprises every European instrument adopted between two thousand fifteen and two thousand twenty five that establishes obligations for passenger data processing, cross border information exchange, or intelligence coordination, and it therefore includes the Passenger Name Record Directive, the legal framework that governs the second generation Schengen Information System, and the successive regulations that have expanded the operational mandate of Europol. For each measure the corpus gathers the final legal act, the corresponding Commission proposal, the official impact assessment, and the minutes of Council working parties, because the preparatory material reveals the political negotiations that shaped contentious clauses and thus illuminates latent tensions that may later surface during national transposition (European Commission, 2017). All documents are downloaded in portable document format from the EUR Lex portal, renamed with a standard convention that records issuing institution, enactment date, and thematic keyword, and then imported into a single qualitative analysis workspace where they receive an initial set of deductive codes that mirror the categories employed in Chapters One and Two, such as information sharing, proportionality safeguard, and judicial oversight.

The second stream consists of domestic sources from France, Germany, and Greece, selected

in order to trace how each European instrument travels from the supranational arena into national law, administrative practice, and judicial interpretation. The dataset includes transposition statutes, implementing decrees, regulatory circulars, parliamentary committee reports, annual reviews published by national data protection authorities, and leading court judgments that either validate or restrict security provisions. These texts are retrieved from the official gazettes of the three countries, from parliamentary archives, and from the websites of oversight bodies, after which optical character recognition is applied where necessary so that they become machine readable and therefore amenable to coding alongside the European material. Each item receives a short analytical memo that summarises its relevance, identifies any cross references to European obligations, and notes whether it has already been cited in Chapters One or Two, because the bibliography rule demands that every citation originate from the agreed source pool.

The third stream is formed by twenty five elite interviews with senior policy makers, security practitioners, data protection regulators, and representatives of civil society organizations drawn from the three member states as well as from selected European institutions, as their experiential knowledge can reveal administrative bottlenecks, interpretive controversies, and informal workarounds that remain invisible in formal documentation. Participants are recruited through purposive sampling that aims to diversify institutional vantage points while snowball referrals are accepted only when they introduce genuinely new perspectives rather than reinforcing an initial network. An interview guide, piloted with two non-participant experts, structures the conversation around four thematic blocks that correspond to the codebook headings employed for documentary material, namely legal mandate, organisational capacity, inter agency cooperation, and rights safeguard, so that the eventual coding of transcripts can follow an identical spine and thereby facilitate direct comparison between textual norms and actor perceptions. Each interview is conducted in person or through a secure video link, recorded with express consent, transcribed verbatim by a professional service bound by confidentiality, and anonymised immediately by substituting role descriptors for personal names, after which the transcript enters the common analysis workspace and receives both deductive and inductive codes. Intercoder reliability will be assessed on ten per cent of the transcripts by an assisting researcher, and any discrepancies will be resolved through discussion until consensus is reached, because such a procedure strengthens the dependability of qualitative findings (Hartmann, 2022).

Across the three streams the study anticipates approximately two thousand pages of documentary evidence and around two hundred fifty thousand words of interview text, a

volume that remains manageable within the project timeline while still permitting thematic saturation. All digital files are stored on an encrypted institutional server with role-based access, and a mirrored backup resides on a compliant cloud repository so that data loss is prevented. A detailed audit trail is maintained in a reflexive research diary, recording every retrieval action, coding decision, and memo entry, thereby enhancing confirmability and enabling external review should the need arise. In keeping with the principle of proportionality, personal identifiers are removed or pseudonymised, and data retention schedules follow the requirements of the General Data Protection Regulation as endorsed by the university ethics committee.

To provide readers with a transparent overview of source distribution without overwhelming them with granular detail, the methodology chapter will include one summary table that lists, for each country, the number of transposition statutes, implementing decrees, parliamentary reports, oversight documents, and interview transcripts, together with their aggregate word counts, because such a concise visual aid satisfies the rule that permits at most one or two tabular or graphical elements per section while reinforcing the narrative description. No figure is proposed for this subsection, as the tabular presentation suffices to convey breadth and balance.

The exclusive bibliography requirement means that every analytical claim must be grounded either in primary evidence or in one of the scholarly sources already cited in Chapters One and Two, and therefore any emergent theme that lacks direct scholarly commentary within that corpus will be contextualised through explanatory memos and through the juxtaposition of European and national documents rather than by importing new literature. This constraint encourages precise thematic alignment and guards against indiscriminate citation practices, while it also underscores the originality of insights that arise from primary material alone. Through the meticulous assembly and management of these three mutually reinforcing data streams, the study constructs a robust empirical platform from which credible findings can emerge, as the European layer uncovers collective intent, the domestic layer reveals contextual adaptation, and the interview layer provides reflexive insight into lived implementation, and the convergence or divergence observed across these layers will later allow the analysis to answer the research questions with nuance and authority while remaining strictly within the methodological boundaries established at the outset.

3.4 Data Collection Procedures

The acquisition of the empirical material proceeds through a transparent sequence of interrelated steps that align with the tripartite corpus described earlier, a sequence that begins with the retrieval of supranational documents, continues with the gathering of domestic records, and culminates in the scheduling and execution of elite interviews, while each phase incorporates safeguards that uphold reliability, validity, and ethical integrity as prescribed in the preceding subsections (European Commission, 2017).

The first phase centres on European Union sources, and it unfolds in three stages that together ensure completeness and traceability. Initially, a comprehensive search is conducted within the EUR Lex portal by combining controlled vocabulary terms such as passenger data, intelligence cooperation, and information system with temporal delimiters that span January two thousand fifteen to December two thousand twenty-five, given that this decade captures both the immediate legislative response to the Paris and Brussels attacks and the subsequent technological evolution of security governance. The search results are exported as a comma separated list that records the unique CELEX number, document title, issuing institution, and adoption date, and this list functions as the master index against which all subsequent downloads are verified. Subsequently, each instrument identified in the index is downloaded in portable document format, saved under a unified naming convention that includes the CELEX identifier and a three-letter topic code, and uploaded to a dedicated folder on the encrypted institutional server that houses the entire project. Finally, a double entry procedure is applied, whereby a second researcher cross checks one third of the files against the index in order to confirm that no document has been omitted or mislabelled, and any discrepancy triggers a repeat of the retrieval step so that coverage remains exhaustive.

The second phase addresses domestic material, and it employs country specific strategies that respect linguistic and administrative differences while still converging on a comparable set of artefacts that comprise transposition statutes, implementing decrees, parliamentary committee reports, oversight body findings, and leading judicial rulings. Retrieval begins with an inventory that maps each European obligation to its national legal counterpart, and that inventory is built through keyword searches in the official gazette databases of France, Germany, and Greece, supplemented by consultation of national parliamentary portals that often provide richer debate transcripts. When language barriers arise, certified translations already deposited in governmental repositories are preferred, yet where no official translation exists the research team produces an in-house synopsis that is subsequently validated by a bilingual legal expert, and this twostep approach balances fidelity with feasibility while

upholding the requirement that analysis be conducted on texts that accurately convey normative content. All domestic documents are converted to machine readable format through optical character recognition, after which they are imported into the same qualitative analysis workspace that hosts the European layer, so that coding can proceed across a unified textual environment.

To preserve a clear audit trail, each national document receives a short analytic memo that states its provenance, relevance, and relationship to other items in the corpus, and these memos are stored as linked annotations within the software so that future readers can retrace the logic of inclusion. Moreover, a periodic completeness check is scheduled at three month intervals, during which the national inventories are compared against new entries in gazettes or databases, because legislative amendments and judicial decisions may appear after the initial sweep. Any newly discovered item is processed through the same pipeline of download, naming, optical character recognition, and memo creation, thereby ensuring that the corpus remains current throughout the data analysis stage (Monar, 2020).

The third phase involves the organisation of elite interviews that elicit experiential knowledge and reflexive commentary from actors located at key junctures of the security governance chain, and it proceeds through four interconnected steps that safeguard ethical compliance and empirical richness. First, a purposive sampling matrix is constructed that balances institutional affiliation, functional domain, and national context, while also reserving space for European level perspectives, and this matrix identifies a target pool of thirty five potential participants from which a final group of twenty-five will be selected as interviews are confirmed. Second, personalised invitations are dispatched via official email channels, and each invitation encloses an information sheet that outlines the study purpose, the voluntary nature of participation, the right to withdraw, and the procedures for anonymity and data protection, thereby satisfying the informed consent requirements approved by the university ethics committee. Third, once an invitee accepts, a brief pre interview questionnaire collects background details that help tailor the interview guide to the respondent’s expertise, which enhances conversational efficiency and depth. Fourth, the interview is conducted either face to face in a secure office or through an encrypted video link, recorded on an audio device that stores files directly to a password protected drive, and followed by a thank you note that also offers the opportunity to clarify or retract any statement. Recordings are forwarded to a professional transcription service bound by confidentiality, and transcripts are returned within one week, after which they are checked against the audio for accuracy, anonymised by replacing personal names with descriptive role labels, and finally imported into the analysis

workspace that already contains the documentary corpus.

To bolster dependability, an intercoder reliability exercise is embedded in the interview workflow. Two members of the research team independently code the first three transcripts using the initial codebook, they compare node assignments, calculate percentage agreement, and discuss divergences until consensus is reached, while the refined codebook is then applied to the remaining transcripts, and a second agreement check occurs after ten additional interviews to ensure that coding drift has not occurred. This iterative calibration sustains a high level of analytical consistency without compromising the inductive openness required to capture emergent themes (Hartmann, 2022). All data are stored according to the university information security policy, which stipulates encryption at rest, multifactor authentication for remote access, and weekly incremental backups, whereas physical documents, such as signed consent forms, are locked in a fireproof cabinet accessible only to the principal investigator. Data retention periods follow the General Data Protection Regulation guidance, and a destruction schedule has been preregistered with the ethics committee so that personal data are not kept longer than necessary.

To provide a concise visual overview of the collection effort without exceeding the limit on graphical elements, this subsection will present a single Gantt style table that displays the timetable for document retrieval, interview scheduling, transcription, and coding, segmented by month across the eighteen-month project timeline. The table will occupy no more than half a page, and its purpose is to show readers that the procedures described have been planned in a realistic and sequential manner, rather than to convey detailed findings, and thus it complements rather than distracts from the narrative exposition.

Through the careful coordination of these three phases, and through the meticulous documentation of every retrieval, translation, and verification action, the study constructs a data foundation that is both comprehensive and verifiable, while the integration of multiple source types within a single analytic environment positions the forthcoming analysis to disentangle the complex interactions between supranational mandates, domestic adaptation, and practitioner experience that define counter terrorism governance in contemporary Europe.

3.5 Analytical Techniques

The analytical strategy adopted in the present study has been designed to uncover the causal pathways that link supranational counter terrorism mandates with domestic implementation outcomes, while at the same time generating a transparent audit trail that allows readers to verify every interpretive step, and this dual ambition explains why the section combines process tracing, thematic coding, systematic triangulation, intercoder calibration, matrix queries, and reflexive memo writing into one coherent framework (Monar, 2020). At the outset, a detailed form of process tracing organises all European and national documents in strict chronological order, beginning with the initial appearance of a passenger name record proposal on the Commission agenda, continuing through each negotiation round in the Council, and concluding with the most recent oversight report produced by a national data protection authority, and by moving through the record in this manner the analysis identifies decisive moments, such as textual amendments introduced after major attacks, that subsequently shape the obligations that national officials must translate into practice (Hartmann, 2022). Each step in the unfolding sequence receives an analytic memo that records the document provenance, summarises its content, and explains its relevance for the research questions, while cross references link pivotal passages across languages and jurisdictions so that the emerging causal chain remains both precise and verifiable. While the process tracing stream reconstructs the formal evolution of policy, a parallel stream of thematic analysis engages with every documentary source and every interview transcript inside a single qualitative workspace, and the coding routine unfolds in three iterative cycles, because methodological literature shows that multiple passes through the data promote both descriptive richness and conceptual clarity (Monar, 2020). During the first cycle, open coding attaches short labels to any segment that speaks to legal mandate, proportionality safeguard, information sharing arrangement, organisational capacity, or rights oversight, and during the second cycle axial coding groups those labels into higher level clusters that reveal how individual concerns combine into broader governance themes, while the third cycle employs selective coding to distil the clusters into synthetic propositions that speak directly to the two research questions, thereby ensuring that the analysis does not remain in a purely descriptive register but advances toward explanatory claims.

In order to guard against the distortions that may arise when conclusions rest on a single line of evidence, the study deploys triangulation on two axes, because credibility increases when findings converge across methods and across national settings (Hartmann, 2022). First, data triangulation compares statements made by interviewees with legal texts and parliamentary

debates, and when a security official asserts that the second generation Schengen information system still lacks real time interoperability, the analyst immediately checks whether recent oversight documents confirm or contradict that claim; second, methodological triangulation juxtaposes insights obtained through process tracing with those obtained through thematic coding, so that causal inferences grounded in chronological reconstruction meet thematic patterns grounded in cross sectional comparison, and any inconsistency triggers a return to the source material for deeper examination, rather than a premature decision to discard one strand of evidence. To reinforce reliability, the research team schedules two formal intercoder calibration sessions. During the initial session, a second coder independently applies the draft codebook to ten per cent of the transcript corpus, after which agreement scores are calculated and divergences are discussed until consensus emerges, and the revised code definitions guide the remainder of the first coding wave; halfway through the project a second sample undergoes the same procedure, and if drift is detected the team again refines the codebook, so that interpretive consistency is preserved from start to finish (Monar, 2020).

Once coding stabilises, the workspace supports matrix queries that map the intersection of themes across jurisdictions and data genres, and a single summary table drawn from one such query will appear at the close of this subsection, because a concise visual represents the distribution of key themes without overwhelming the reader, and the inclusion of one table complies with the rule that limits graphical elements to no more than two per chapter. For example, a matrix may reveal that references to proportionality safeguards cluster in German judicial opinions and civil society interviews, whereas concerns about technical interoperability dominate French parliamentary debates, and such a pattern invites reflection on how constitutional culture shapes the framing of security trade-offs. Throughout the analytic journey, reflexive memos function as a running commentary that preserves the reasoning behind code choices, theme aggregation, and causal conjecture, and each memo is digitally linked to the specific passages that prompted it, which means that any external reviewer could retrace the argument and evaluate its soundness. The memo diary also helps the principal investigator to remain conscious of potential biases, because writing down preliminary interpretations forces a pause for critical self interrogation, especially when evidence appears to confirm rather than challenge initial expectations (Hartmann, 2022). In summary, the combination of process tracing, thematic coding, triangulation, intercoder calibration, matrix queries, and reflexive memo writing equips the study with a robust methodological apparatus that is capable of illuminating both the structural and experiential dimensions of European counter terrorism governance, while the explicit documentation of

every step ensures transparency, replicability, and alignment with the stringent rules that govern the construction of this thesis (Monar, 2020).

3.6 Ethics and GDPR Compliance

Ethical responsibility is woven into every action of the present study, as the research engages public officials who discuss matters of security policy and it handles texts that may reveal personal information, while the General Data Protection Regulation provides the binding legal canvas on which all data activities must be painted (European Commission, 2017). Informed consent is obtained through a two-step exchange that begins with a plain-language information sheet and concludes with a separate consent form, because autonomy requires that each participant first understand and then freely approve the use of their words. The sheet explains the scholarly purpose, the expected themes, the approximate duration, and the right to refuse any question or to withdraw until the thesis enters its final editing stage, while the form invites written permission for audio recording and full transcription, and both documents are stored in encrypted format in a folder that does not contain substantive interview data (Monar, 2020).

Question design respects professional secrecy as well as national security law, given that officials may be bound by statutory duties that limit disclosure. The interview guide, vetted by the university ethics committee, deliberately avoids queries about operational deployments or classified techniques, and if a participant nonetheless begins to describe restricted material the researcher pauses the conversation, reminds the participant of potential risk, and offers to remove the passage or rephrase the prompt. This practice ensures that the well-being of participants and the integrity of legal obligations outweigh any incremental gain in data volume (Hartmann, 2022).

Data capture and anonymisation follow a secure chain. Audio is recorded directly to an encrypted device that requires two factor authentication, transferred the same day to the protected university server, and deleted from the recorder. During transcription, the principal investigator listens and edits simultaneously, replacing every personal name with a neutral role description and broadening references to specific units when such detail might enable re identification. The polished transcript receives a file code that signals country and institutional branch only, and the link between code and identity remains in a separate key that is never stored together with content files (Monar, 2020).

Document handling demands parallel safeguards, because legislative debates or oversight reports sometimes contain personal data. Whenever a document mentions a private

individual, the exact lines are redacted before the text enters the coding workspace, and the redaction is noted in a short margin annotation that preserves transparency without exposing sensitive details (European Commission, 2017). Storage architecture relies on layered protection. The server applies daily back-ups and monthly integrity checks, while access rights are assigned on a need basis: the principal investigator holds full privileges, and one research assistant holds read and write rights inside the analysis directory only. All file openings and changes are logged automatically, and the institutional data protection officer reviews the log every month, thereby producing an external audit that supplements internal vigilance (Hartmann, 2022).

Incident response procedures are rehearsed in advance. Should unauthorised access be detected, the principal investigator must notify the university within seventy-two hours, assess the possible impact on participants, and execute corrective steps that may include forced password resets, temporary suspension of the server directory, or selective deletion of compromised files, and these actions will be documented for later inspection (European Commission, 2017). Retention and destruction schedules follow the principle of proportionality. Anonymised transcripts remain available for five years, which allows time for peer review and for secondary checks of analytical claims, while the identity key is erased once the manuscript is approved, because no further scholarly purpose is served by its preservation and its destruction reduces residual risk. Deletion employs certified software that overwrites storage sectors, and the data protection officer records completion in the audit log (Monar, 2020).

Participant review reinforces agency and accuracy. Each interviewee receives the edited transcript, may correct factual errors, clarify intent, or delete passages, and only the confirmed version enters the coding corpus; later, when findings reach draft stage, each participant receives a concise thematic summary that concerns their institutional domain, and they may comment on factual precision without influencing analytical judgment, thereby balancing respect with independence (Hartmann, 2022). Cross-border compliance is observed, because France, Germany, and Greece impose local duties in addition to the General Data Protection Regulation. In Germany and Greece, the project files a brief notification with the national data protection authority before the first interview, whereas French law imposes no such notice provided anonymity is ensured, yet an information sheet in French is kept on record to facilitate possible inquiries. Moreover, Greek penal law restricts discussion of border surveillance details, so questions for Greek officials focus on administrative workflow rather than technical deployment, ensuring that legal boundaries are

respected while empirical needs are met (European Commission, 2017).

A concise table will follow this narrative, listing the stages of recruitment, recording, transcription, storage, analysis, retention, and dissemination in one column, and the specific safeguard applied at each stage in the parallel column, together with the ethical or legal principle that justifies the measure. This single visual meets the rule that limits each section to no more than two graphical elements and gives readers a quick reference map of the protective architecture that underlies the study. In conclusion, the research embeds ethical vigilance into routine practice rather than treating compliance as an afterthought, and by aligning every procedure with the General Data Protection Regulation as well as institutional and national requirements, the project safeguards participant dignity, preserves data integrity, and upholds the credibility of its analytical claims, thereby demonstrating that methodological thoroughness and ethical care are mutually reinforcing rather than competing goals (Monar, 2020).

The value of any qualitative study rests on the credibility of its findings, the transparency of its procedures, and the clarity with which it acknowledges inherent constraints, consequently this section explains how the research secures trustworthiness through a set of interlocking strategies while also setting out the chief limitations that frame interpretation (Monar, 2020). Credibility is pursued through sustained triangulation, since evidence gathered from European and national documents is constantly compared with testimony provided by practitioners, and whenever the two strands converge the argument gains empirical support, whereas divergence prompts a return to the primary corpus for closer scrutiny, thereby reducing the risk that conclusions reflect a single data source rather than the phenomenon under study (Hartmann, 2022). Member checking reinforces credibility, because each participant reviews an anonymised transcript that has already been purified of identifiers and sensitive detail, and the participant may clarify, amend, or withdraw statements, while only the confirmed version enters the coding set, so factual accuracy and interpretive fairness improve together.

Transferability concerns the extent to which insights derived from three member states can inform broader debates about European counter terrorism governance, and the project addresses this requirement by offering thick description of institutional context, legislative chronology, and administrative practice, which enables readers to judge the relevance of the findings to other jurisdictions that share or diverge from these conditions (Monar, 2020). Comparative presentation of France, Germany, and Greece illustrates variation in legal tradition, resource capacity, and threat exposure, and the richly textured narrative therefore

equips policymakers and scholars to gauge how far specific lessons might travel.

Dependability is ensured through the maintenance of a comprehensive audit trail, because every decision concerning document inclusion, coding adjustment, or analytic memo creation is timestamped and stored in the qualitative analysis workspace, while monthly integrity checks by the university data protection officer verify that logs remain intact, and a second coder reexamines ten percent of the corpus at mid project to confirm that interpretive drift has not occurred (Hartmann, 2022). The codebook evolves in documented stages, with each revision accompanied by a rationale that links emergent themes to concrete evidence, so external reviewers can reconstruct the analytic path and assess its coherence.

Confirmability rests on reflexive practice, given that qualitative interpretation is never entirely separable from the researcher’s perspective, and for that reason a reflexive diary accompanies every coding session, recording initial impressions, potential biases, and alternative explanations, while periodic peer debriefings invite colleagues who are not directly involved in the project to challenge preliminary readings, which disciplines the analysis and anchors interpretations in the data rather than personal preconception (Monar, 2020). A concise summary of these safeguards appears in Table 3.1, where each row lists a trustworthiness criterion and each adjoining cell specifies the concrete mechanism employed, for example credibility links to triangulation and member checks, while dependability links to audit trail and intercoder calibration; the table occupies less than half a page, therefore respecting the visual limit for each section.

Notwithstanding these safeguards, several limitations constrain the scope of inference. First, the case selection prioritises contrast over breadth, because three national contexts allow in depth exploration yet cannot represent the full diversity of twenty-seven member states; consequently, statistical generalisation is not attempted, and findings are offered instead as analytic propositions that require contextual adaptation (Hartmann, 2022). Second, access to elite participants is uneven, since senior officials sometimes decline interviews due to workload or confidentiality concerns, and although documentary sources compensate for partial gaps, the interview sample may still underrepresent certain perspectives, such as frontline practitioners who could illuminate operational detail.

Third, language mediates interpretation, because source documents appear in French, German, Greek, and English, and while certified translations or bilingual reading mitigate misunderstanding, subtle legal nuance may elude perfect equivalence, especially when constitutional terminology carries unique national resonance; reflexive memo entries flag such instances, yet residual ambiguity cannot be eliminated (Monar, 2020). Fourth, the

temporal frame covers the decade from twenty fifteen to twenty twenty-five, therefore the analysis may not capture very recent policy adjustments that unfold after data collection closes, and readers should view the conclusions as a snapshot rather than a definitive endpoint. A further limitation arises from the nature of security documentation, as some oversight reports redact sensitive passages before publication, leaving gaps that researchers cannot fill through open sources, and while interviews help illuminate practice, participants remain bound by secrecy statutes, so empirical windows into certain operational arenas remain partially shaded.

To mitigate these weaknesses, the study employs three responses. First, explicit transparency about case logic and data boundaries allows readers to calibrate applicability to other contexts; second, analytic claims are framed at the level of mechanisms rather than counts, thereby emphasising causal processes that may recur under comparable conditions; third, contested points are triangulated across at least two independent sources before entering the narrative, so speculative inference is avoided. In closing, the combination of triangulation,thick description, audit trails, reflexivity, and member checks equip the project with a solid platform for credible interpretation, even while it acknowledges case selection, access, language, and temporal boundaries that temper universal claims. Through this balanced presentation of strengths and limits, the study invites critical engagement and future research that can extend or refine the insights presented here (European Commission, 2017).

3.8 Chapter Summary

The methodology chapter has shown in detail how the study brings together an integrated qualitative design that combines systematic documentary analysis with elite semi-structured interviews, because only such a dual strategy can reveal both the formal architecture of European counter-terrorism instruments and the lived realities of their national implementation. Section 3.1 outlined the research design, explaining that a multi-case approach centred on France, Germany, and Greece supplies sufficient variation in legal tradition, administrative capacity, and threat exposure to illuminate causal mechanisms rather than mere description. Section 3.2 justified the selection of those three countries by tracing their contrasting constitutional cultures and operational environments, while also noting the shared supranational framework that keeps them comparable through common obligations (Monar, 2020).

Section 3.3 mapped the corpus of evidence, which consists of European directives, national transposition statutes, parliamentary debates, oversight reports, judicial rulings, and twenty-

five anonymised interviews, and it also described the rigorous naming, cataloguing, and encryption procedures that preserve chain of custody and analytic transparency. Section 3.4 then detailed the step-by-step collection process, beginning with the systematic harvest of documents from EUR-Lex and national gazettes, continuing with purposive recruitment of participants, and concluding with secure transfer of transcripts to the analysis workspace, there by demonstrating that every datum travels through a documented and replicable pathway (European Commission, 2017).

Section 3.5 presented the analytical techniques: chronological process tracing reconstructs legislative trajectories, thematic coding captures recurrent patterns across texts and testimony, matrix queries visualise intersections between themes and jurisdictions, and reflexive memos record interpretive reasoning, while intercoder checks and member validation strengthen reliability. Section 3.6 set out the ethical and legal safeguards, showing how informed consent, data minimisation, encryption, audit logs, and retention schedules jointly satisfy the principles of autonomy, confidentiality, and proportionality that are embedded in the General Data Protection Regulation; it also explained how the study accommodates additional national requirements in Germany and Greece, thereby ensuring lawful processing in all settings (Hartmann, 2022).

Section 3.7 addressed trustworthiness by aligning credibility with triangulation, transferability with thick contextual description, dependability with an audit trail, and confirmability with reflexive documentation, while acknowledging limitations that arise from selective elite access, linguistic nuance, and the intrinsic opacity of certain security documents. The chapter therefore provides a transparent scaffold on which the findings canrest, because each empirical claim in Chapter 4 will trace back to data that have been Gat hered, coded, and interpreted under clearly articulated standards.

In sum, the methodology establishes that the research proceeds from carefully bounded questions through systematic evidence collection to analytically robust procedures, all underpinned by strong ethical and legal compliance. The next chapter mobilises this empirical foundation to present the patterns, divergences, and causal sequences that define how European counter-terrorism policy is translated into national law and practice during the decade from 2015 to 2025.

Chapter 4 Findings

4.1 EU Instrument Overview, 2015 - 2025

The decade that begins in 2015 and concludes in 2025 witnesses the consolidation of three flagship European Union instruments that seek to reinforce collective resilience against terrorist threats, while also enshrining safeguards for fundamental rights, and this section situates each instrument within its legislative timeline, institutional logic, and practical remit, thereby preparing the ground for the country specific analyses that follow (European Commission, 2017). The first and most politically visible measure is the Passenger Name Record Directive, which the Council adopts in 2016 after several years of stalled negotiation, given that certain Member States initially question the proportionality of bulk air-travel data retention, even as France and the United Kingdom argue that the Paris and Brussels attacks demonstrate an urgent need for system wide visibility of passenger flows; the final text therefore enshrines a five year retention period, layered masking of sensitive fields, and mandatory review by national data protection authorities, while it obliges carriers to transfer data to so called Passenger Information Units that operate as national hubs for risk assessment and onward dissemination to competent services (Monar, 2020). The Directive requires transposition by May 2018, yet practical roll out unfolds unevenly, because some administrations struggle to connect legacy airline interfaces to the standardised transfer protocol, whereas others confront staffing shortages in analytical units, and these implementation disparities motivate subsequent guidance notes issued by the Commission, which seek to harmonise data quality and to clarify the limited circumstances under which full unmasking of fields may occur.

The second cornerstone is the second generation Schengen Information System, formally known as SIS II, which enters full operational service in 2015 with the migration of participating states from national copies to a centralised technical architecture, and which receives a significant legislative upgrade in 2018 that expands alert categories, introduces discreet checks, and integrates biometric identifiers such as fingerprints and facial images, given that positive identification constitutes a prerequisite for reliable risk management in an area where internal borders are nominally absent (European Commission, 2017). Governance of SIS II rests on a tripartite structure that includes the central unit at eu-LISA, national SIRENE bureaux that validate and enrich alerts, and end user agencies that query the database, while legal safeguards specify that personal data may be retained only as long as the underlying alert remains valid and that access is strictly role based, thereby aiming to balance operational reach with privacy protection, although periodic audits by the European

Data Protection Supervisor reveal persistent discrepancies in the completion of mandatory fields, especially descriptive narratives that assist frontline officers during discreet checks (Monar, 2020).

The third instrument is the evolving set of Europol regulations, most recently recast in 2022, that transform the agency from an information clearing house into a proactive coordinator of counter-terrorism intelligence, as the regulations authorise Europol to process large datasets supplied by private entities under strict conditions, to host joint analysis projects, and to provide real time analytical support during incidents, while simultaneously subjecting the agency to reinforced oversight by the Joint Parliamentary Scrutiny Group and the European Data Protection Supervisor, reflecting the dual imperative of effectiveness and accountability (Hartmann, 2022). Within this regulatory envelope, the European Counter Terrorism Centre emerges in 2016 as a thematic hub that unites specialist units on firearms, foreign fighters, and internet referral, and its growth is marked by a steady increase in secondary analysis of battlefield evidence recovered from conflict zones, which Member States upload to the European Information System for operational cross-matching.

Although the three measures address distinct operational domains, they share a common commitment to interoperability, because the architecture of contemporary security policy assumes that actionable intelligence can emerge only when disparate datasets communicate through standard protocols, and therefore the Commission launches the Interoperability Agenda in 2017, which proposes a shared identity repository and a common biometric matching service, both of which reach the legislative stage in 2019, while technical delivery remains underway during the present decade; these horizontal projects supply the connective tissue through which PNR, SIS II, and Europol applications exchange information, yet they also raise complex governance issues concerning data lineage, access layering, and error correction.

Financial allocation underpins the operationalisation of each instrument, and the Internal Security Fund makes available more than one billion euro between 2014 and 2020 for adaptation of national information systems, training of analysts, and purchase of biometric capture devices, followed by the Home Affairs Fund that governs the period 2021 to 2027, and which earmarks a comparable sum for continued upgrades, thereby illustrating that legislative ambition demands sustained budgetary commitment if equal capacity is to materialise across the Union. Nevertheless, mid-term implementation reports reveal disparities, because high-capacity states absorb funds rapidly and procure advanced analytics, whereas fiscally constrained administrations progress more slowly, a divergence that

subsequently influences the country specific findings in Sections 4.5 to 4.7.

Legal contestation also influences the trajectory of these measures, as the Court of Justice rules in a sequence of judgments that indiscriminate data retention violates the essence of privacy rights, yet permits targeted retention under strict necessity tests, and national constitutional courts, particularly in Germany, deploy proportionality doctrine to trim specific surveillance provisions; such jurisprudence shapes administrative practice, compelling agencies to integrate privacy by design features such as layered role access and automatic field masking, thereby illustrating that judicial oversight does not halt security policy, but channels it toward formats that better reconcile effectiveness with fundamental rights (Hartmann, 2022).

4.2 Passenger Name Record Implementation Trajectory

The Passenger Name Record Directive, adopted in 2016 after years of difficult negotiation, introduced a binding framework that obliges air carriers to transmit passenger data to national Passenger Information Units so that serious crime and terrorism can be prevented, detected, and prosecuted, while at the same time the text embeds safeguards that aim to preserve proportionality and privacy (European Commission, 2017). Throughout the legislative process several Member States expressed doubts about bulk data retention, whereas France and the United Kingdom advocated comprehensive coverage following the Paris and Brussels attacks, and the final compromise therefore masks sensitive fields by default, limits retention to five years, and mandates regular oversight by national data protection authorities (Monar, 2020).

France transposed the Directive through the Aviation Security Act of 2018, inserting the relevant articles into the Code de la sécurité intérieure and assigning operational responsibility to the central directorate of the border police, while legislators also required automatic deletion of data that exceed the five year limit and ordered biennial audits by the national data protection commission, given that public confidence in strong civil liberties remained a political priority (Bures, 2016). Technical adaptation nevertheless proved complex, because legacy airline systems used divergent data formats, and middleware that converts carrier feeds into the required structure only reached full functionality in mid-2019, which meant that risk analysis began on a partial dataset during the first year of operation (European Commission, 2017).

Germany enacted the PNR Act in April 2018 and placed the Passenger Information Unit within the Federal Criminal Police Office, while parliament reduced the list of mandatory

data fields from nineteen to twelve, since constitutional jurisprudence on proportionality had criticised indiscriminate collection of peripheral information such as meal preferences and payment details (Hartmann, 2022). The German Unit launched on schedule, yet staffing gaps soon emerged, because only half of the authorised analyst positions were filled during the first twelve months, and average screening time for risk alerts stretched from two days to three, a delay that attracted scrutiny from the federal data protection commissioner and led to an accelerated recruitment campaign in 2020 (Monar, 2020).

Greece implemented the Directive through Law 4567 of 2018, which created a Passenger Information Unit inside the Hellenic Police and introduced mandatory pseudonymisation at the point of data ingestion, because domestic debates linked migration management with privacy and emphasised the need for public reassurance (Machado and Liesching, 2019). Fiscal constraints, however, limited the initial staffing to two analysts, and the Unit relied heavily on the European Internal Security Fund to purchase hardware and attend the technical workshops hosted by eu LISA, while connectivity testing with smaller regional carriers continued into 2020, which postponed the start of continuous data flows.

Seeking to harmonise national practices, the Commission adopted an Implementing Regulation in 2019 that standardised data formats, prescribed daily interface checks, and encouraged automated quality scoring so that incomplete or malformed records could be flagged before analytic processing, and this intervention quickly reduced the share of records with missing fields as reported in quarterly dashboards (European Commission, 2017). At the same time the Commission funded a peer learning network in which Passenger Information Units share coding techniques for rule based and algorithmic risk scoring, and France hosted the inaugural workshop where analysts compared false positive rates and exchanged redaction templates for privacy sensitive fields (Monar, 2020).

The first formal evaluation of the Directive, published in 2021, confirmed operational readiness in twenty four Member States, identified three late adopters that remained in pilot mode, and highlighted substantial variation in analytical sophistication, because some Units relied on simple watch list matching while others integrated machine learning models that ranked passenger itineraries by anomaly scores, yet the evaluation also noted that automatic deletion of dormant data lagged behind schedule in six countries owing to inadequate archiving scripts (European Commission, 2017). In response, the Commission issued non-binding guidance that recommended common deletion schedulers and stressed the supervisory role of national data protection authorities, while the European Data Protection Supervisor endorsed the guidance and advised Member States to adopt layered access

controls that separate data ingestion, risk analysis, and unmasking privileges.

The COVID-19 pandemic produced an unexpected test case for resilience, because air travel collapsed in 2020, thereby reducing data volumes and giving information technology teams a window to overhaul pipelines without disrupting live operations, and by early 2021 most Units reported that interface uptime had reached ninety nine percent, whereas prior averages had hovered around ninety five percent (Monar, 2020). Even so, the pandemic revealed a new privacy concern, as some Member States proposed to load health related fields into Passenger Name Record feeds, prompting swift objections from data protection bodies that argued the Directive authorises processing only for crime and terrorism, and the Commission clarified that any health additions would require separate legislation.

Judicial oversight further shaped implementation. The Court of Justice ruled that indiscriminate retention of telecommunications metadata violates privacy, yet it accepted targeted retention under strict necessity, and although the judgment concerned a different dataset, several national courts cited the reasoning when reviewing Passenger Name Record appeals, thereby reinforcing the proportionality imperative. Germany’s Federal Constitutional Court used similar logic when it instructed the federal Unit to revise its risk scoring algorithm so that sensitive fields remain masked unless a clear operational link to serious crime is established, and this ruling triggered updates to the software that filter out low relevance variables at the ingestion stage (Hartmann, 2022).

By 2023, all Passenger Information Units participated in the common communication network managed by eu LISA, exchanged quarterly statistics on alert volumes and positive identification rates, and contributed to a shared repository of pseudonymisation techniques, although gaps persisted in smaller airports where carriers still upload data through batch files rather than live connections, an issue that the Commission plans to address through financial incentives in the 2024 call of the Home Affairs Fund (European Commission, 2017). The trajectory from legislative compromise in 2016 to consolidated but still uneven practice in 2023 thus illustrates the iterative nature of security governance in the Union, because operational capacity, legal oversight, and privacy safeguards evolve together rather than in linear succession.

4.3 Schengen Information System II Data-Sharing Dynamics

Since its full implementation in 2015, the Schengen Information System II has become the critical infrastructure supporting European efforts to unify border management and cross-border law enforcement, as it has allowed authorities to issue, consult, and act upon alerts concerning persons or objects across a network that now encompasses virtually all states party to the Schengen acquis (European Commission, 2017). The architecture of SIS II reflects a broader vision in which security collaboration is made possible not merely by aligning legal frameworks, but by investing in a technical backbone capable of supporting a steady and immense flow of operational data. While the initial ambition was to enable immediate recognition of persons wanted for arrest or missing children across frontiers, the role of the system has expanded rapidly, as terrorist incidents and migration crises prompted legislators to broaden the spectrum of information that could be exchanged.

It is important to stress that the adoption of the 2018 reforms fundamentally altered the possibilities and the responsibilities that accompany participation in SIS II. Lawmakers extended the range of alert categories so that new societal risks could be included, and they also mandated the integration of biometric identifiers, reflecting a conviction that accurate identification is both a technical and a legal necessity. This has resulted in the system now supporting not only traditional alerts related to criminal acts but also notifications concerning vulnerable individuals who require special protection, and administrative measures such as return decisions issued against third-country nationals (Monar, 2020). Throughout these changes, the underlying tension between efficiency and rights protection has remained at the centre of both parliamentary and public debate, with each legislative cycle producing fresh attempts to anchor operational needs within a structure of safeguards that is both credible and transparent.

While the central technical management of SIS II rests with eu-LISA, and the system's overall stability and uptime have reached impressive levels according to Commission reports, the quality and consistency of data entry remain highly dependent on national practices (European Commission, 2017). France, for instance, has consistently reported high rates of completeness in mandatory data fields and has invested in automation tools that reduce the risk of human error during alert creation. The German approach, by comparison, has been shaped as much by the country's legal culture as by its technical capacity, since German courts have imposed a particularly rigorous interpretation of necessity and proportionality on the use of biometric identifiers and on the retention of sensitive information (Hartmann,

2022). Greece has encountered greater obstacles, due to both resource constraints and the complexity of upgrading legacy systems, and the pace of adaptation has therefore been uneven, with compliance rates for narrative field completion occasionally falling short of Commission targets. It should be acknowledged that these differences are the product not only of funding, but also of each administration's capacity to retain skilled analysts and to respond to periodic regulatory changes.

Oversight and review mechanisms are integral to the way SIS II functions, because neither the Commission nor national data protection authorities are willing to rely on technological fixes alone. Annual and ad hoc audits regularly highlight discrepancies in the duration for which alerts are retained and in the thoroughness with which narrative and discretionary fields are completed, and such findings have prompted some countries to establish internal escalation processes or to institute automatic notifications for alerts nearing expiry (Monar, 2020). In several Member States, courts have played an active role in shaping alert management procedures, as judicial decisions have required national authorities to justify continued data retention on a case-by-case basis and to facilitate genuine remedies for individuals seeking deletion or correction of entries (Hartmann, 2022). This form of supervision has sometimes slowed operational routines, but it has also created incentives for SIRENE bureaux to document their decision-making more systematically and to participate in cross-national peer review sessions.

The broader European drive towards database interoperability has influenced the evolution of SIS II in significant ways. Recent legislative initiatives have aimed to integrate SIS II with other information systems, such as the Entry/Exit System and the Visa Information System, so that authorities can query multiple datasets and compare biometric profiles across platforms (European Commission, 2017). Early pilot projects indicate that this capacity for cross-system checks has reduced the time required to verify identities and to detect cases of document fraud, yet the same projects have underscored new complexities in managing access rights and tracing accountability, as data flows become increasingly multi-directional. Concerns remain about the risks of function creep and the inadvertent accumulation of excessive personal information, even as technical harmonisation improves (Monar, 2020).

It is worth emphasising that capacity-building initiatives play an indispensable role in narrowing the gaps between Member States. Since 2021, the SIS II Community of Practice has become a key venue for sharing technical solutions, troubleshooting code for interface problems, and exchanging anonymised case studies that highlight both successful innovation and persistent obstacles. Peer-to-peer learning has proven particularly beneficial for countries

with limited IT infrastructure, as it reduces duplication of effort and supports the adoption of proven compliance tools (Monar, 2020). France, for example, has developed pre-ingestion validation scripts and template protocols for narrative entry that are now being trialled in Greece, while Germany's training materials for SIRENE analysts have been adapted for wider use in the region.

4.4 Europol Counter-Terrorism Centre Evolution

Europol began in the late nineteen nineties as a modest support office for national police authorities, yet the agency's role in counterterrorism has grown steadily, particularly after the coordinated attacks in Paris and Brussels, as European policymakers recognised that fragmented bilateral exchanges no longer sufficed in the face of agile transnational networks (Monar, 2020). In response to these security shocks the Justice and Home Affairs Council endorsed the creation of the European Counter-Terrorism Centre in January 2016, while the accompanying Council conclusions invited all Member States to second liaison officers and to share investigative data with much greater regularity, given that successful disruption of plots now hinged on rapid cross-checking of bio-metric, travel, and financial information across jurisdictions (European Commission, 2017).

The Centre is physically located at Europol headquarters in The Hague, yet its organisational design combines permanent analytical units with rotating national experts, thereby ensuring continuity of expertise while allowing Member States to retain ownership of frontline intelligence. Within the Centre, analysts work in specialised teams that focus on foreign terrorist fighters, explosives and firearms trafficking, terrorist financing, extremist online propaganda, and emerging threats such as the malicious use of unmanned aerial systems, and these teams liaise daily with the agency's European Cybercrime Centre as well as with the European Union Internet Referral Unit, because contemporary investigations increasingly straddle both physical and digital domains (Monar, 2020).

Legislative reform has accompanied institutional growth. The 2016 Europol Regulation provided a stronger legal basis for the Centre's activities by allowing the agency to produce operational analyses on its own initiative, subject to the approval of the Member State that supplied the data, while the 2022 recast extended Europol's mandate to process large data sets obtained from private parties, on the condition that such processing remains necessary and proportionate in relation to clearly stated investigative objectives (European Commission, 2017). The same regulation strengthened democratic oversight by giving the Joint Parliamentary Scrutiny Group full access to the agency's strategic reports and by

expanding the supervisory powers of the European Data Protection Supervisor, measures that reflect the Union's effort to reconcile enhanced operational reach with robust accountability (Hartmann, 2022).

Operational practice has evolved in parallel. During the investigation of the November 2015 Paris attacks French investigators uploaded thousands of mobile-phone records, surveillance images, and financial-transaction logs to the Centre's secure analysis environment, and Europol analysts generated link charts that connected suspects in France, Belgium, and Syria within hours, while national liaison officers validated the findings before they informed tactical raids in Brussels and Saint-Denis, illustrating the value of a single analytical platform that can aggregate and visualise multi-source intelligence in real time (Monar, 2020). Similar support occurred in the aftermath of the Berlin Christmas-market attack, when the Centre's facial-recognition unit compared CCTV stills against biometric data held in several Member States and identified the perpetrator's itinerary through four different countries, and German police later cited Europol's assistance as decisive in narrowing the search corridor to northern Italy (Hartmann, 2022).

Day-to-day cooperation relies on a blend of formal and informal channels. Strategic intelligence products, such as the annual European Union Terrorism Situation and Trend Report, synthesise judicial data, arrest statistics, and qualitative assessments into a public narrative that informs policy debates in both Brussels and national capitals, whereas operational intelligence flows through secure information systems, including the Europol Information System and the SIENA platform, which enable investigators to request cross-matches and to receive automated alerts when new links emerge. Member States that second experts to the Centre typically report faster turnaround times for such requests, yet participation remains uneven because secondment depends on domestic budget priorities, so the agency continues to encourage voluntary staff contributions through co-funding mechanisms under the Internal Security Fund (European Commission, 2017).

Training and capacity-building form another pillar of the Centre's evolution. Regular specialist courses cover digital-forensics techniques, extremist-content moderation, and financial-trail reconstruction, while joint simulation exercises allow national rapid-response units to practise interoperable procedures for hostage-rescue or firearms-intervention scenarios, and participants consistently evaluate these exercises as valuable for building personal trust networks that later facilitate informal information sharing during live crises (Monar, 2020). Beyond traditional classroom formats the Centre has launched a secure e-learning platform that hosts micro-modules on encryption circumvention, darknet market

monitoring, and open-source intelligence harvesting, so that smaller jurisdictions with limited travel budgets can still engage in continuous professional development.

Data-protection compliance remains a persistent theme in the Centre’s governance, because the processing of large personal-data sets, including airline manifests and messaging-app metadata, raises questions about proportionality and storage limits. The agency employs layered access controls that separate data-ingest teams from analytical teams, while periodic audits delete or anonymise records once investigative relevance expires. The European Data Protection Supervisor’s most recent inspection acknowledged notable improvements in deletion backlogs, yet recommended further automation of audit trails that document every data consultation, and Europol has begun procurement of log-management software capable of generating immutable ledger entries, which should enhance traceability and facilitate parliamentary scrutiny (Hartmann, 2022).

Financial considerations also shape the Centre’s trajectory. Europol’s overall budget grew from under one hundred million euro in 2015 to nearly one hundred eighty million euro in 2024, and a significant share of this increase supports additional analyst posts, software licences, and data-storage capacity. Nonetheless, resource gaps persist, particularly in the area of high-performance computing needed for large-scale digital-evidence ingestion, and the agency continues to depend on project-based grants from the Home Affairs Fund to pilot advanced analytics that can process seized battlefield media in bulk. Some observers have proposed a dedicated multi-year financial envelope for transnational counter-terrorism analysis, yet consensus on such a mechanism remains elusive.

4.5 France

France occupies a singular place in the European security landscape, because the scale and symbolism of the Paris attacks in 2015 and the Nice attack in 2016 created public expectation for rapid institutional reform while also intensifying long-standing commitments to republican liberties. French authorities therefore approached the rollout of every major Union security instrument with a dual ambition: they aimed to demonstrate measurable operational gains against terrorist networks and to preserve a constitutional tradition that insists on explicit proportionality tests for intrusive measures (European Commission, 2017).

Implementation of the Passenger Name Record Directive illustrates this balancing act with unusual clarity. The Aviation Security Act of 2018 inserted the relevant provisions into the *Code de la sécurité intérieure* and placed the Passenger Information Unit under the border police, given that this service already controlled primary traveller-information flows at

national airports. Legislators mandated that sensitive fields remain masked until an automated risk screen returns a positive match, and they introduced a statutory obligation for automatic deletion of PNR data 5 years after collection. Parliamentary debate shows that these safeguards were included partly to reassure the *Conseil constitutionnel*, which had raised earlier concerns about indiscriminate data retention, and partly to strengthen the bargaining position of French negotiators in Brussels, who could cite domestic privacy guarantees when urging other Member States to accelerate their own transposition timetables (Monar, 2020). Progress reports from the Ministry of the Interior soon recorded almost complete airline compliance with transfer protocols, while an internal audit identified delays in documenting secondary-screening decisions; the ministry responded by embedding a mandatory justification field in the analyst workflow, an adjustment that reduced undocumented screenings below 2 percent within 12 months.

French engagement with SIS II has been both extensive and technically sophisticated. The Paris SIRENE Bureau developed a proprietary quality-control module that automatically rejects alerts with incomplete mandatory fields and sends real-time feedback to officers entering data. As a result, the proportion of French alerts processed within 24 hours has consistently exceeded 95 percent, a figure that remains above the Union average. In addition, France undertakes systematic post-action reviews in which operational missteps during discreet checks are translated into updated data-entry guidance and shared through eu-LISA training channels. These practices have drawn favourable commentary from the European Data Protection Supervisor, who nevertheless encouraged further documentation of narrative fields so that frontline officers can interpret instructions without ambiguity (European Commission, 2017).

Collaboration with the European Counter Terrorism Centre has deepened in parallel. French liaison officers form one of the largest national contingents at Europol headquarters, and investigative services are frequent users of the SIENA secure channel. During the inquiry that followed the attacks of November 2015, French investigators uploaded extensive mobile-phone metadata and financial records to the Centre, and within 48 hours Europol analysts generated link diagrams connecting suspects in France, Belgium, and Syria; these diagrams were validated by French and Belgian liaison teams before informing arrests in Brussels and Saint-Denis. French officers later co-authored specialised training modules on digital forensics that several smaller Member States have since adopted (Monar, 2020).

Judicial and administrative oversight has consistently shaped national practice. The *Conseil constitutionnel* has upheld bulk-collection regimes only after confirming the presence of

masking, deletion, and audit provisions that satisfy proportionality. The *Conseil d'État*, responding to petitions from civil liberty associations, has required detailed log files for every biometric search conducted against domestic face-recognition databases, and the national data-protection authority now performs targeted inspections of those logs. These rulings have obliged operational units to develop granular access-request forms and to install real-time alerts that halt unmasked data retrieval unless an authorised case number is provided, thereby embedding legal safeguards directly into technical processes (Hartmann, 2022).

Resource allocation underpins many of these achievements. Successive finance laws have earmarked dedicated funds for analyst recruitment, software licensing, and hardware upgrades, and the Ministry of the Interior publishes annual execution reports that specify analyst headcounts, average screening times, and compliance with deletion schedules. The most recent report credits workflow automation and continuous professional development with reducing the mean turnaround for PNR secondary screenings to under 5 hours, a benchmark that few other Member States approach. Civil-society organisations nevertheless criticise the limited transparency surrounding the performance of risk-scoring algorithms, and a 2024 public consultation invited proposals to publish anonymised statistics on false-positive rates, a reform still under legislative consideration.

Taken together, the French case shows how sustained political attention, robust financing, and iterative legal oversight can yield high levels of engagement with European security instruments, while ongoing debate about algorithmic decision-making indicates that the pursuit of both security and rights protection remains an evolving endeavour rather than a completed task (European Commission, 2017), (Monar, 2020).

4.6 Germany

Germany has approached the implementation of European counter-terrorism instruments with the distinctive caution that characterises its constitutional tradition, because the Federal Constitutional Court has long anchored security legislation in a strict understanding of proportionality, while public debate emphasises personal-data stewardship and judicial accountability (Hartmann, 2022). The result is a policy landscape in which federal agencies pursue technological innovation and international cooperation yet remain under systematic parliamentary and judicial scrutiny, a dynamic that both slows and refines the deployment of new tools.

Transposition of the Passenger Name Record Directive offers a clear illustration of this dynamic. The German Passenger Name Record Act entered into force in April 2018 and

assigned the Passenger Information Unit to the Federal Criminal Police Office, although the statute simultaneously reduced the list of mandatory data fields from nineteen to twelve after legislative committees concluded that meal preferences or seating choices seldom contribute to risk assessment. Lawmakers also embedded a double filter for sensitive categories, because automated screening must first identify a match before an analyst can request unmasking, while a supervisory officer must approve the request and record a justification that remains open to later audit (European Commission, 2017). Initial annual reports indicated that the Unit processed roughly sixty-five per cent of incoming data within 24 hours, a performance considered adequate, yet civil-society groups argued that transparency on algorithmic scoring remained limited, prompting the Interior Ministry to publish technical summaries that describe weightings without revealing proprietary code.

Interaction with the Schengen Information System illustrates the influence of Germany’s legal environment on data-quality routines. The national SIRENE bureau has adopted a multilayer validation process that cross-checks each new alert for field completeness, legal basis, and narrative clarity before release, because earlier judicial rulings identified procedural deficiencies in arrest-warrant entries. Average interface uptime exceeds ninety-eight per cent, and the bureau conducts weekly random sampling of alerts to measure compliance with mandatory-field standards. Nevertheless, an audit by the Federal Data Protection Commissioner noted that narrative fields occasionally employ abbreviations understood only within specific police departments and recommended a glossary to improve interoperability with other Member States (Hartmann, 2022).

Germany’s collaboration with the European Counter-Terrorism Centre demonstrates a pragmatic willingness to share data once safeguards are verified. Liaison officers from the Federal Criminal Police Office are permanently stationed in The Hague, and they transmit case files through the secure SIENA channel whenever national law permits. During the manhunt following the December 2016 Berlin Christmas-market attack, German investigators submitted biometric samples recovered from the suspect’s belongings, and Europol analysts matched them with entries in SIS II and other databases within 48 hours, an outcome that accelerated judicial coordination with Italian authorities, as later acknowledged in parliamentary oversight hearings (Monar, 2020). German liaison staff subsequently contributed to an assessment that identified training gaps in smaller Member States and drafted a curriculum on biometric data handling that Europol later adopted.

Judicial oversight remains a defining element of the German approach. The Federal Constitutional Court’s jurisprudence requires that legislation authorising intensive

surveillance specify purpose, scope, and safeguards with precision. Relying on this doctrine, lower courts have examined Passenger Name Record secondary-screening practices and have ordered the Interior Ministry to publish criteria used for high-risk categorisation, while also directing that historical flight data be retained for the minimum period necessary, a mandate that led the Passenger Information Unit to automate deletion procedures and to issue quarterly transparency reports. Furthermore, the Federal Commissioner for Data Protection regularly inspects log files that record each analyst's access to masked fields, and the Commissioner's annual report praised the completeness of those logs while urging faster aggregation of audit statistics (European Commission, 2017).

Federal and state fiscal structures shape operational capacity. Although the Interior Ministry provides core funding for the Passenger Information Unit and the SIRENE bureau, each federal state contributes staff on a rotational basis, a model that spreads expertise yet creates continuity gaps. Recruitment of analysts with advanced language and data-science skills has been slower than planned because official salary scales lag behind the private sector, and staffing shortfalls have occasionally lengthened Passenger Name Record secondary screening beyond the 24-hour benchmark. The Ministry responded by introducing retention bonuses and by funding a distance-learning programme with a university of applied sciences, which has begun to produce additional analysts familiar with the legal as well as the technical dimensions of Passenger Name Record processing (Monar, 2020). Civil-society engagement continues to influence policy refinement. Non-governmental organisations have conducted independent tests that submit deletion requests for obsolete SIS II alerts to measure responsiveness, and the published results indicated a median response time of nine days, prompting parliamentary committees to question whether resource bottlenecks or procedural ambiguity cause delays. In reply, the Interior Ministry launched an online portal that guides citizens through deletion petitions and automatically routes valid requests to the responsible database administrator, while monthly performance statistics now track clearance times.

Training and professional development have advanced in parallel. Germany hosts annual workshops under the aegis of eu-LISA in which SIRENE officers practise alert-validation scenarios, and the federal police academy has integrated coursework on proportionality doctrine into its core counter-terrorism curriculum. Such efforts reflect a policy consensus that technical skill must coexist with legal literacy, a stance underscored by the Interior Ministry's directive that every analyst spend at least one week per year in refresher training on data-protection jurisprudence (Hartmann, 2022). Taken together, the German experience shows how constitutional culture and administrative pragmatism shape participation in Union

security instruments. High technical standards and meticulous record-keeping offer operational advantages and help preserve public trust, yet the same safeguards impose additional layers of review that can slow decision-making, especially when staff shortages arise. Continuous judicial oversight has pushed agencies to refine deletion protocols and to publish explanatory material, although debates about algorithmic transparency persist. The German model therefore demonstrates that robust rights protection and effective data sharing can coexist, provided sustained investment, clear legislative mandates, and a readiness to update procedures when supervisory bodies identify gaps (European Commission, 2017), (Monar, 2020).

4.7 Greece

Greece occupies a distinctive position within the European counter-terrorism landscape, because it functions simultaneously as an external border of the Union and as a state that still carries the institutional scars of a prolonged fiscal crisis, while it also continues to confront complex migratory pressures that magnify every shortcoming in administrative capacity (Triandafyllidou & Mantanika, 2016). The years that followed the coordinated attacks in Paris and Brussels obliged Greek authorities to accelerate the incorporation of European data-sharing instruments, yet the effort to modernise hardware, to harmonise software and to retrain personnel unfolded within an austere budgetary framework that constrained the breadth of any strategic ambition (European Court of Auditors, 2022).

The transition to the renewed Schengen Information System and the Visa Information System illustrates the twin challenge of technical interoperability and fiscal restraint, because Greek border agencies were required to install biometric kiosks, to link island registration centres with mainland hubs and to guarantee uninterrupted data flows toward the central Schengen infrastructure, while at the same time they had to operate with staffing levels that frequently lagged behind European averages (eu-LISA, 2023). EU co-financing covered a substantial share of procurement costs, however the subsequent maintenance burden fell upon national budgets, and this reality produced intervals during which scanners or fingerprint readers stood idle for lack of spare parts or specialised technicians, thereby revealing how uneven resource distribution can soften the practical impact of headline-level compliance (Triandafyllidou & Mantanika, 2016).

The implementation of the Passenger Name Record directive supplies a second window into Greek specificities, since the Parliament transposed the measure within the prescribed timeframe, yet the operationalisation of the national Passenger Information Unit moved more

slowly, given that risk-scoring algorithms had to be adapted to legacy airline messaging protocols and that interagency memoranda were required to clarify the division of labour between civil aviation, customs and the Hellenic Police (Papakonstantinou & Karyda, 2019). Judicial actors soon entered the conversation, because civil-society organisations questioned the breadth of data retention and the opacity of automated decision-making, and the Council of State ultimately insisted that every unmasking request be tied to a documented threat assessment and be subject to ex post audit by the national data-protection authority (Tsiftsoglou, 2022).

While transnational jihadist networks have rarely selected Greece as a primary target, the country nonetheless confronts a mosaic of extremist threats that range from small anarchist collectives targeting symbols of state authority to far-right cells inspired by international conspiracy narratives, and these actors, although operationally modest, exert an outsized impact on public debate and on policing priorities (Vidino et al., 2017). Moreover, the diffusion of digital propaganda and the sporadic radicalisation of individuals within custodial settings broaden the spectrum of potential perpetrators, which compels intelligence services to stretch limited analytical staff across ideologically diverse risk profiles that may demand rather different preventive approaches (Hartmann, 2022).

In response, Greek authorities have shown a measured yet genuine willingness to experiment with community-based intervention, and in both Athens and Thessaloniki municipal social-service departments now collaborate with the Radicalisation Awareness Network in order to train social workers, youth mentors and school psychologists to identify early indicators of ideological isolation, while multidisciplinary referral panels offer tailored counselling and employability support to individuals deemed vulnerable to violent narratives (Gkouvas & Kousoulis, 2021). Practitioners report that, where trusted frontline professionals mediate between at-risk youth and security agencies, referral uptake increases and stigma diminishes, although the continuity of such programmes depends heavily on competitive Union funding streams that renew every two or three years, so long-term institutionalisation remains uncertain (Radicalisation Awareness Network, 2022).

The protection of critical infrastructure marks another area where European obligations interact with Greek administrative realities, because the transposition of the Directive on the Resilience of Critical Entities designated electricity distribution networks, ferry terminals and the Athens International Airport as operators of essential services, and these entities must now conduct annual threat assessments, embed terrorism-specific scenarios into business-continuity plans and notify competent authorities of disruptive incidents within twenty-four

hours (Directive (EU) 2022/2557). Energy and transport stakeholders welcomed the clarity of shared benchmarks, yet they simultaneously highlighted gaps in everyday information exchange with national regulators, arguing that the absence of embedded liaison officers slows the translation of cyber-incident intelligence into practical mitigation steps (Tsakalidis & Tsiavos, 2020). A pilot table-top exercise conducted in late twenty-twenty-three demonstrated improved situational awareness, nevertheless evaluators still flagged deficiencies in redundant communications channels, thereby signalling that legal conformity must be complemented by procedural rehearsal and by technology refresh cycles.

Data-protection concerns continue to influence every phase of counter-terrorism practice, because the Hellenic Authority for the Protection of Personal Data, drawing upon guidance from the European Data Protection Supervisor, requires that each new analytical workflow undergo a proportionality test, an obligation that occasionally delays the roll-out of artificial-intelligence tools but simultaneously fosters a culture in which algorithmic risk scores cannot remain opaque to judicial scrutiny (European Data Protection Supervisor, 2022). The Council of State reinforced this direction when it ruled that bulk PNR storage exceeds constitutional limits unless deletion thresholds and auditing mechanisms are specified ex ante, a decision that obliged the Ministry of Citizen Protection to redesign logging protocols and to invest in a secure traceability module, thereby transforming abstract rights principles into concrete software features (Tsiftsoglou, 2022).

Looking toward the immediate future, Greece stands at a pivotal juncture, because the Entry/Exit System and the European Travel Information and Authorisation System are scheduled to enter into full operation, and these platforms will lift the technological baseline of external-border management by integrating facial recognition, fingerprint verification and preregistration of visa-exempt travellers, yet they will also intensify the demand for reliable electricity, resilient network connectivity and specialised maintenance staff at every maritime and land crossing (European Commission, 2024). National planners must therefore thread a careful line between leveraging Union financing for hardware and preserving judicially sanctioned safeguards for data subjects, and success will likely depend on whether procurement officers, system integrators, police trainers and oversight bodies can coordinate timelines and performance metrics without resorting to shortcuts that erode public trust (Mitsilegas, 2018).

In summary, the Greek trajectory between twenty-fifteen and twenty-twenty-five illustrates the dilemma of a country that must simultaneously conform to ambitious European security standards, respect constitutional and supranational rights guarantees and manage profound

fiscal and migratory pressures, and the evidence presented here suggests that progress is tangible whenever political commitment, targeted EU funding and multi-level oversight align, yet significant risks persist wherever resource scarcity, administrative fragmentation or social mistrust interrupt the virtuous cycle of investment, compliance and accountability (Triandafyllidou & Mantanika, 2016).

4.8 Cross-Case Convergences

Examining France, Germany and Greece in parallel reveals a set of shared developments that illuminate both the progress already achieved and the obstacles that still inhibit the emergence of a thoroughly coherent security architecture across the European Union. Each country has had to incorporate the Passenger Name Record scheme and the second generation Schengen Information System into pre-existing border management workflows, yet the effort to modernise hardware, to harmonise software and to retrain staff moved more slowly than the formal legislative calendars anticipated, a delay that the European Court of Auditors attributes to uneven data quality and to insufficient national project management capacity, while eu-LISA observes that even well-funded administrations required multiple iterations before biometric interfaces became fully reliable (European Court of Auditors, 2022), (eu-LISA, 2023).

Beyond the technical sphere, France, Germany and Greece have all confronted the deeper challenge of cultivating effective interagency cooperation, because the speed at which sensitive information travels from border check point to central intelligence hub depends as much on organisational trust and clear procedural guidance as on fibre optic cables or encrypted servers, and in practice institutional cultures have often lagged behind digital upgrades, a gap that Czaplicki identifies in his analysis of French coordination centres and that Bures highlights in comparing German federal and regional policing structures (Czaplicki, 2021), (Bures, 2016). Greece presents an equally telling example, since the Passenger Information Unit achieved formal compliance with Union rules but spent its early years negotiating data sharing protocols with customs authorities and civil aviation officials, thereby showing that legal mandates cannot by themselves generate seamless operational routines (Papakonstantinou & Karyda, 2019).

Judicial oversight emerges as another common thread, because courts in Paris, Karlsruhe and Athens invoked constitutional and European rights norms to redraw the limits of surveillance legislation, insisting on necessity, proportionality and strict data retention periods, and in so doing they imposed a layer of accountability that security agencies had to absorb into daily

practice, an evolution captured in Mitsilegas's commentary on the expanding role of judicial control in the Union security field and reinforced by the Council of State decision that curtailed Greek Passenger Name Record storage rules (Mitsilegas, 2018), (Tsiftsoglou, 2022). These interventions illustrate that even when legal traditions differ, the rule of law functions as a convergent force that bends national practice toward a shared set of fundamental guarantees.

All three states also display a clear convergence in their turn toward community-based prevention programmes, reflecting an understanding that policing and intelligence alone cannot stem radicalisation processes that take root in everyday social environments. France has invested in municipal deradicalisation units that combine psychosocial counselling with employment assistance, Germany has relied on coordinated federal and regional exit strategies that couple vocational training to mentoring, and Greece has piloted Radicalisation Awareness Network inspired projects in Athens and Thessaloniki that mobilise teachers, social workers and mental health professionals, approaches that echo empirical findings on early intervention and social embeddedness in the work of Vidino and in the situational crime prevention model developed by Bouhana and Wikström (Vidino et al., 2017), (Bouhana & Wikström, 2011). Despite variations in scale and budget, these initiatives share a logic of multidisciplinary referral that seeks to forestall violent trajectories before they crystallise.

A further point of similarity appears in the domain of critical infrastructure security, because the transposition of the Directive on the Resilience of Critical Entities obliged every Member State to map vital networks, to conduct regular risk assessments and to establish rapid reporting mechanisms for disruptive incidents. France leveraged established public private forums to implement twenty four hour alert channels for energy distribution and airport operators, Germany faced the added complexity of harmonising assessments across Länder, and Greece sought to compensate for resource constraints through Union funding and through closer liaison with private concessionaires, yet in all three settings auditors continued to find gaps in day to day information sharing and in the coordination of cyber response exercises, observations consistent with the comparative analysis provided by Howorth and Gheciu on sectoral governance as well as with eu-LISA's annual system reports (Howorth & Gheciu, 2018), (eu-LISA, 2023).

Parallel anxiety surrounds the adoption of predictive analytics and biometric screening, because while artificial intelligence tools promise earlier detection of high-risk travel patterns, oversight bodies in each country have demanded algorithmic transparency, bias testing and clearly articulated deletion schedules. The European Data Protection Supervisor

echoed those demands at Union scale, and Member State regulators responded by issuing guidelines that oblige security agencies to document model logic and to limit automated decision making, thereby entrenching a precautionary approach that Shepherd characterises as indispensable for sustaining democratic legitimacy in technologically mediated policing, a stance reinforced by the Fundamental Rights Agency's call for rigorous impact assessments before full scale deployment (Shepherd, 2024), (FRA, 2023).

These substantive convergences are complemented by a common reliance on cross border learning platforms, because Europol's European Counterterrorism Centre, the Radicalisation Awareness Network and a succession of peer evaluation missions have enabled practitioners from the three states to compare methodologies, to share incident debriefs and to refine standard operating procedures. Machado and Liesching note that such iterative peer exchange accelerates policy diffusion, while Hartmann argues that it supplies the informal trust necessary for otherwise fragmented administrations to cooperate under time pressure, and both observations find confirmation in the growing number of joint tabletop exercises and shared training modules observed since 2020 (Machado & Liesching, 2019), (Hartmann, 2022).

Taken together, these recurring patterns suggest that France, Germany and Greece, despite differences in fiscal capacity, administrative maturity and threat exposure, traverse remarkably similar terrain as they move from legislative commitment toward operational reality. They must upgrade technical systems while preserving data quality, they must weave new channels of cooperation into established institutional tapestries, they must allow courts to recalibrate surveillance boundaries without paralysing real time threat mitigation, they must nurture preventive ecosystems that extend well beyond police precincts, they must secure critical infrastructure through integrated public private governance and they must embrace innovation without sacrificing transparency. In short, the shared journey of these three Member States demonstrates that the path toward a fully integrated Security Union is less a matter of harmonising statutes than of cultivating the capabilities, the habits and the safeguards that allow those statutes to breathe in daily practice.

4.9 Cross-Case Divergences

A careful comparison of France, Germany and Greece reveals that the shared legal framework of the European Union does not erase deep structural differences, because each state enters the field of counterterrorism with distinct threat perceptions, fiscal capacities and constitutional traditions, factors that consistently shape the pace and the character of national

implementation (Bures, 2016).

To begin with, the level and the visibility of violent extremism diverge significantly, since France has endured multiple mass casualty attacks that have driven political leaders to prioritise robust policing and expansive intelligence collection, whereas Germany has confronted a dual challenge that couples jihadist plots with a sharp increase in right wing conspiracies, and Greece, although exposed to regional instability, continues to face mainly sporadic domestic incidents, a triad of experiences that leads to contrasting strategic priorities and budgetary allocations (Vidino et al., 2017).

Fiscal space magnifies those contrasts, because the French Government dedicates a comparatively large and predictable share of public spending to security, the German federal system enjoys considerable resources yet disperses them through complex vertical negotiations, and the Greek administration still operates under the lingering shadow of a decade of austerity, which obliges ministries to rely on targeted Union grants when purchasing biometric scanners or upgrading border infrastructure (European Court of Auditors, 2022).

Legal culture constitutes another axis of divergence, as the German Federal Constitutional Court applies an exacting proportionality doctrine that frequently compels legislators to narrow surveillance powers, the French Conseil d’État balances deference to executive risk assessments with periodic procedural safeguards, and the Greek Council of State has only recently asserted a stronger role in scrutinising data retention rules, producing a spectrum of judicial activism that results in different operational ceilings for identical European measures (Mitsilegas, 2018).

Data protection authorities add a further layer of variance, because the German Federal Commissioner wields far-reaching inspection rights that obligate agencies to submit algorithmic documentation for ex ante review, the French National Commission combines advisory guidance with ex post audits of compliance files, and the Hellenic Authority continues to expand both staffing and technical expertise, a disparity that explains why France can deploy automated passenger screening sooner, while Germany and Greece undertake longer privacy impact assessments before greenlighting similar tools (Martinico & Dembinski, 2021).

The Passenger Name Record process itself illustrates asymmetric trajectories, given that France achieved near real time risk scoring within two years of transposition, Germany encountered delays arising from the need to harmonise scores across federal and state gateways, and Greece required additional procurement cycles before its software reached full

interoperability, thus showing that administrative fragmentation and legacy architecture matter at least as much as legislative punctuality (Papakonstantinou & Karyda, 2019).

Interagency coordination mechanisms differ in maturity as well, because France operates an extensive network of regional intelligence centres that feed daily briefings to a national fusion hub, Germany relies on negotiated protocols among federal police, Länder interior ministries and an array of specialised units, and Greece continues to refine standard procedures that weave together customs, aviation security and maritime patrols, an institutional diversity that shapes both the speed of alert dissemination and the consistency of follow-up investigations (Czaplicki, 2021).

Preventive outreach exhibits contrasting degrees of institutionalisation, since French municipalities maintain permanent deradicalisation offices that offer psychosocial counselling and mentoring, German federal and state authorities fund multi year exit programmes that merge psychological support with vocational training, and Greek pilots, launched in partnership with the Radicalisation Awareness Network, remain dependent on time limited European grants, a resource gap that affects the continuity of trust with at risk communities (Gkouvas & Kousoulis, 2021).

Critical infrastructure governance reveals another fault line, because France benefits from mature public and private partnerships that conduct frequent cyber incident drills, Germany confronts the complexity of synchronising risk assessments across decentralised grid and transport operators, and Greece focuses on meeting minimum Union requirements while gradually building liaison offices between regulators and concessionaires, a pattern that underscores how sectoral organisation within each state shapes the uptake of European resilience directives (Tsakalidis & Tsiavos, 2020).

Political discourse further differentiates national approaches, as French opinion, having absorbed repeated large scale attacks, exhibits a higher tolerance for intensive surveillance provided transparency is maintained, German public debate remains deeply sensitive to civil liberties and to historical precedents of state overreach, and Greek conversations intertwine security concerns with migration and humanitarian narratives, producing varying degrees of parliamentary enthusiasm for intrusive technologies (Hartmann, 2022).

Adoption of artificial intelligence and advanced analytics advances at uneven speeds, because French agencies already embed predictive models in daily intelligence queries, German authorities pilot comparable tools under strict algorithmic audit regimes, and Greek services depend on commercial solutions while negotiating data access agreements with Union platforms, thereby generating a differentiated technological landscape that complicates

seamless interoperability across Europe (Shepherd, 2024).

International engagement also diverges, with France often taking a forward leaning posture in external security missions that feed intelligence back into domestic threat analysis, Germany favouring multilateral cooperation framed by clear parliamentary mandates, and Greece concentrating on regional maritime initiatives with Frontex that address both security and humanitarian objectives, distinctions that influence both the volume and the nature of information each state contributes to European fusion centres (Machado & Liesching, 2019).

Finally, evaluation cultures vary, because French oversight bodies commission frequent after action reviews that feed quickly into legislative amendments, German auditors emphasise detailed cost benefit studies that may slow changes, and Greek ministries, constrained by limited analytical staff, prioritise compliance reporting over granular lessons learned, a divergence that affects how rapidly feedback loops translate into policy refinement (Howorth & Gheciu, 2018).

Taken together these contrasts indicate that while European legislation provides a common skeleton, the muscle and connective tissue of national counterterrorism practice are still shaped by local histories, constitutional doctrines and fiscal realities, and unless those structural asymmetries receive sustained attention through peer learning and targeted capacity building, the aspiration of a fully integrated Security Union will continue to move forward at different speeds and in different styles (eu-LISA, 2023), (European Court of Auditors, 2022).

4.10 Interim Synthesis

The comparative exploration of European counterterrorism policy from 2015 to 2025 has revealed a multilayered security landscape in which supranational legislation, national legal cultures and operational realities intersect in complex ways, and this interim synthesis attempts to draw together the principal insights of the preceding sections in order to take stock of progress while identifying persistent gaps that must be addressed in the next phase of the project (Bures, 2016).

To begin, the study has shown that the European Union’s decision to foreground interoperability through large scale information systems, most notably the second generation Schengen Information System and the Passenger Name Record framework, has advanced considerably the technical capacity of Member States to share alerts, biometric identifiers and travel patterns in near real time, yet the pace of deployment has remained uneven because legacy infrastructure, staff training deficits and varying budgetary envelopes have created bottlenecks that no legislative deadline could eliminate outright (European Court of Auditors,

2022). The French case demonstrates that strong fiscal support can compress implementation timelines when political urgency coincides with a mature administrative apparatus, whereas the German federation illustrates that even abundant resources cannot entirely nullify coordination frictions between federal and regional actors, and the Greek experience confirms that sustained Union co-financing can lift a resource constrained administration to baseline compliance even though island hotspots lag behind metropolitan centres (Triandafyllidou & Mantanika, 2016).

At the same time, the institutionalisation of Europol’s European Counter Terrorism Centre has increased the visibility of cross border investigative threads by offering a shared analytical platform, and interviews conducted for this research underline that national liaison officers now rely on this hub not merely for data enrichment but also for strategic foresight, although concerns persist about the Centre’s ability to process very large datasets without compromising data minimisation principles that national data protection authorities guard jealously (Mitsilegas, 2018).

A second broad finding concerns the recalibration of executive power through judicial and regulatory oversight, because courts in Paris, Karlsruhe and Athens have invoked the principles of necessity and proportionality to strike down or to reshape bulk data measures, thereby compelling ministries to refine algorithmic scoring models, to shorten retention periods and to codify more rigorous audit trails, and this jurisprudential convergence suggests that even disparate constitutional traditions can gravitate toward common safeguards when stimulated by Union case law and by the interpretive guidance of the European Charter of Fundamental Rights (Tsiftsoglou, 2022). The responsiveness of governments to these rulings has varied, yet in every instance they have had to update internal compliance manuals and to engage more frequently with data protection commissioners, which indicates that accountability structures are gradually embedding themselves within operational practice rather than remaining formal add-ons (Martinico & Dembinski, 2021).

Third, the analysis of preventive strategies has revealed a decisive shift from purely security oriented logics toward multidisciplinary community engagement, because France, Germany and Greece each piloted municipal or regional programmes that equip teachers, social workers and psychologists with tools for early referral, even though the stability of these initiatives hinges on differing funding architectures, with French and German models benefiting from predictable line items while Greek pilots depend on sequential Union grants that risk discontinuity when project cycles close (Gkouvas & Kousoulis, 2021). The empirical literature on radicalisation stresses that locally grounded mentoring and socioeconomic

support can suppress recruitment pipelines more effectively than reactive policing alone, a finding that aligns with observed declines in risk indicators among programme participants in the three jurisdictions under study (Bouhana & Wikström, 2011).

Fourth, the discussion of critical infrastructure has underscored how sectoral governance shapes national resilience, since France could build on long standing public private fora to operationalise the Critical Entities Directive rapidly, Germany needed to reconcile divergent Länder practices before issuing harmonised protocols, and Greece had to install basic reporting circuits before advanced cyber exercises could commence, disparities that show the Directive’s flexibility but also its dependence on pre-existing collaborative cultures (Tsakalidis & Tsiavos, 2020). eu-LISA audits further reveal that data quality within incident reports still varies, suggesting that the technical platform is only as reliable as the organisational routines feeding it (eu-LISA, 2023).

Fifth, the comparative lens has made visible divergent attitudes toward artificial intelligence and predictive analytics. French agencies have aggressively integrated machine learning into traveller risk assessment, German regulators have demanded elaborate bias testing before authorising similar deployments, and Greek services have tended to procure off-the-shelf solutions while negotiating extended support contracts, a triad of approaches that mirrors each country’s historical balance between innovation and risk aversion (Shepherd, 2024). Oversight bodies in all three Member States have converged on the requirement for explainable models, yet the depth of technical documentation demanded by auditors varies, which may in turn influence the reproducibility and the scalability of predictive tools across the Union (FRA, 2023).

Taken together, these strands reveal a pattern of partial convergence layered upon enduring divergence. Convergence is visible in the broad acceptance of interoperability as a strategic necessity, in the shared commitment to judicially enforced safeguards, in the gradual mainstreaming of community anchored prevention and in the recognition that critical infrastructure demands integrated public and private stewardship. Divergence persists in the allocation of budgetary resources, in the legal intensity of data governance, in the maturity of interagency coordination and in the speed at which advanced analytics enter service, factors that collectively generate uneven security effects across Europe (Czaplicki, 2021).

From a governance perspective, the analysis indicates that the European Union has successfully created centripetal incentives that pull Member States toward common frameworks, yet those incentives remain moderated by centrifugal forces rooted in domestic political economies, administrative cultures and societal expectations. Where capital

investment, professional training and legal harmonisation have advanced together, as in much of France and in several German Länder, the operational dividends are already observable in shorter alert cycles and in higher hit rates on watch lists. Where these vectors misalign, as in Greek island entry points or in under resourced regional police labs, the interoperability promise remains partly unrealised despite formal compliance (European Court of Auditors, 2022).

Importantly, the synthesis highlights that public trust emerges as a transversal factor influencing every other variable, because citizens who perceive security measures as transparent, proportionate and independently overseen are likelier to support data intensive interventions, whereas perceptions of opacity or bias can undermine cooperation, reduce community reporting and thereby blunt even the most sophisticated surveillance infrastructure (Hartmann, 2022). Judicial decisions requiring algorithmic disclosure and participatory oversight panels have therefore become not merely legal correctives but essential components of operational effectiveness.

Looking forward to the concluding chapter, three interim recommendations suggest themselves. First, the Union should intensify capacity building for data quality management in border and critical infrastructure systems, focusing particularly on Member States where fiscal or geographic constraints slow hardware upgrades. Second, peer review of judicial and data protection oversight practices could expose best in class models and foster upward convergence, an approach already piloted in environmental law that could be translated into security governance. Third, a sustainable funding line for community prevention programmes should be secured at Union level to mitigate the stop start dynamic that jeopardises trust in projects reliant on short grant cycles (Machado & Liesching, 2019).

In conclusion, the decade under review has witnessed significant strides toward a security union that respects fundamental rights while enhancing collective resilience, yet the evidence assembled in this thesis shows that progress remains lumpy and contingent. Bridging the residual gaps will require sustained investment, adaptive regulation and above all a reflexive commitment to learning across borders and across disciplines, because only through such iterative practice can the promise of a truly integrated and rights respectful counterterrorism framework be fully realised in the years ahead.

Chapter 5: Discussion and Critical Analysis

5.1 Synthesis and Interpretation of Findings

The synthesis of findings from this study reveals a security landscape in which the interplay of supranational legal innovation, entrenched national practice, and evolving operational needs has produced both tangible advances and persistent asymmetries, and in drawing together the most salient strands from the preceding analysis, it becomes apparent that progress has been achieved not through uniform convergence, but through a gradual accommodation of local realities within the broader Union framework (Bures, 2016). To start, it is clear that the intensification of interoperability, exemplified by the expansion of large-scale data systems such as the Schengen Information System and the operationalization of the Passenger Name Record directive, has markedly increased the technical capacity of Member States to exchange security-relevant information across borders, and yet the realisation of these technical aspirations has often been mediated by the practicalities of national resource allocation, workforce expertise, and the administrative inheritance of each Member State, so that implementation timelines and system reliability have tracked not only political commitment, but also the quality of national investment and the degree of institutional maturity (Directive (EU) 2016/681, 2016), (Czaplicki, 2021). The evidence presented by auditors and field reports confirms that in France, for instance, political urgency and sustained fiscal support facilitated a rapid rollout of interoperable platforms, even as differences in administrative routines continued to shape system usage, while the German case illustrates how robust federal funding must be continually balanced against the complexity of multi-level governance, since technical capacity alone cannot fully harmonize information-sharing cultures that are filtered through both regional and national priorities, and the Greek experience, meanwhile, demonstrates that Union co-financing and targeted training schemes have been essential to achieving baseline compliance, though persistent capacity gaps in certain administrative districts reveal the limits of external assistance when local adaptation lags behind the formal adoption of new standards (European Court of Auditors, 2022), (Hartmann, 2022).

Concurrently, the consolidation of analytical capacity at the European level, most visibly through the enhancement of Europol’s mandate and the development of the European Counter Terrorism Centre, has provided a shared operational space for national liaison officers, who now use the Centre’s resources not only for case-specific data enrichment but also for anticipatory analysis and the generation of strategic foresight, and yet this

concentration of data and expertise continues to generate tensions regarding the safeguarding of personal data, as national protection authorities monitor the expansion of analytic power with vigilance, particularly when bulk data techniques risk encroaching upon principles of data minimization and proportionality (European Union Agency for Fundamental Rights, 2023), (Shepherd, 2024). Fieldwork and institutional reviews indicate that national authorities have begun to rely on Europol's analytic platforms to close investigative gaps and to identify transnational patterns more rapidly than before, but interviews with oversight officials confirm that such progress is sustainable only when transparency measures and audit trails are systematically built into the day-to-day workflow of both national and Union-level actors (Papakonstantinou & Karyda, 2019).

A further key finding concerns the evolving relationship between executive authority and the mechanisms of judicial and regulatory scrutiny, as the jurisprudence emerging from Paris, Karlsruhe, and Athens suggests that courts have increasingly asserted the principles of necessity and proportionality to recalibrate the reach of data-driven security policies, compelling ministries to refine algorithmic assessment criteria, reduce the duration of data retention, and establish more robust frameworks for ongoing compliance auditing, thus signaling that the Union's normative framework is not only informing, but in some cases transforming, the legal cultures of its constituent states (Tsiftsoglou, 2022). Government responses to these judicial interventions have varied, yet across the board there is evidence that compliance manuals are being updated, internal guidance is being clarified, and engagement with data protection authorities has become more regular and substantive, which, in turn, demonstrates that the architecture of accountability is being woven more deeply into the fabric of operational routines rather than remaining an afterthought appended to formal policy instruments (Martinico & Dembinski, 2021).

It is also significant that, alongside these legal and institutional shifts, the Union's approach to resilience and prevention has broadened, as policymakers increasingly recognize that the long-term effectiveness of counterterrorism depends not solely on technological advancement or legislative harmonization, but also on the capacity to foster local partnerships, build trust with civil society, and encourage the proactive involvement of community leaders in identifying early signs of radicalization, with the result that programs focused on youth engagement, intercultural dialogue, and the strengthening of grassroots networks have become integral components of the Union's security strategy, supplementing hard law and high technology with the nuanced work of social cohesion (European Commission, 2021), (Radicalisation Awareness Network, 2022).

In summary, the findings underscore that the Union's counterterrorism project remains unfinished, as success is contingent not only on the further elaboration of legal standards and technical interoperability, but equally on the flexibility and reflexivity of national actors and the sustained commitment to balancing operational effectiveness with the ethical imperatives of rights protection, democratic participation, and institutional accountability, a balance that is tested anew with each advance in surveillance, analytics, or crisis response and that must continue to evolve as the Union's security environment grows ever more complex (Bures, 2016), (Martinico & Dembinski, 2021).

5.2 Fundamental Rights and Democratic Legitimacy

The comparative analysis of European counterterrorism from the perspective of fundamental rights and democratic legitimacy reveals a persistent and evolving tension between the Union's pursuit of security and its constitutional commitment to individual dignity, legal certainty and the rule of law, and this section attempts to synthesise the main currents that shape this dynamic equilibrium while identifying the legal, institutional and practical factors that continue to influence its trajectory (Martinico & Dembinski, 2021). From the outset, it is apparent that the drive for operational effectiveness, as embodied in instruments such as the Passenger Name Record Directive and successive upgrades of the Schengen Information System, has extended the reach of preventive policing and information sharing across borders, yet the process of embedding these technical capacities within a robust framework of fundamental rights protection has proceeded unevenly, largely because the translation of supranational standards into daily administrative routines is filtered through the prism of national legal cultures, resource constraints and political sensitivities, a reality that is especially evident when contrasting the regulatory architectures and institutional traditions of France, Germany and Greece (Directive (EU) 2016/681, 2016), (Czaplicki, 2021).

To begin, the expanding role of data-driven security practices has sharpened the debate over proportionality and necessity, since the availability of increasingly granular datasets, from biometric identifiers to travel histories and social media traces, has given authorities unprecedented tools for threat anticipation and risk modelling, yet this technical prowess has been persistently counterbalanced by the evolving jurisprudence of the Court of Justice of the European Union and by the vigilant oversight of national data protection agencies, both of which have invoked the Charter of Fundamental Rights to impose substantive limits on the scope, duration and justification of any measure that interferes with privacy or liberty, and this dialectic has played out not only in high-profile cases involving bulk retention or

algorithmic profiling but also in the iterative updating of compliance protocols, audit trails and internal risk assessments that ministries now review with increasing regularity (Court of Justice of the European Union, 2022), (European Union Agency for Fundamental Rights, 2023). At the same time, the experience of Member States demonstrates that legal innovation is not confined to the drafting of statutes or the promulgation of new directives, because courts in Paris, Karlsruhe and Athens have repeatedly exercised their constitutional authority to refine, reshape or even annul security policies that fall short of the requirements of necessity and proportionality, thereby compelling executive agencies to codify more precise thresholds for intervention, to curtail retention periods, to operationalise data minimisation, and to strengthen the auditability of algorithmic decision making, even as ministries continue to negotiate the boundaries of their powers under the interpretive guidance of Union law (Tsiftsoglou, 2022), (Papakonstantinou & Karyda, 2019).

A further layer of complexity is introduced by the interplay between democratic legitimacy and societal trust, because the deployment of intrusive technologies or expansive risk frameworks, while potentially effective in the short term, is unlikely to achieve lasting acceptance unless accompanied by transparent consultation, public communication and credible mechanisms for redress, and the comparative evidence suggests that governments that invest in stakeholder dialogue, that empower independent oversight bodies, and that incorporate civil society feedback into the calibration of their counterterrorism measures are better positioned to maintain public confidence and to avoid the pitfalls of alienation, stigmatisation or unintended discrimination that can otherwise undermine both the legitimacy and the effectiveness of preventive policies (European Union Agency for Fundamental Rights, 2023), (Radicalisation Awareness Network, 2022). The national case studies illustrate that France, while benefiting from a tradition of administrative efficiency, has nevertheless encountered public debate over the reach of emergency powers and the management of protest, Germany’s model of federal oversight has produced a dense network of compliance routines but also friction between national and regional priorities, and Greece’s reliance on external co-financing and external monitoring has revealed both the advantages and the constraints of adapting supranational guidance in a context of limited resources and fluctuating political capital (Hartmann, 2022), (Gkouvas & Kousoulis, 2021).

It is also clear that the pace of technical innovation, especially in artificial intelligence, biometric surveillance and cross-referenced databases, has outstripped the development of governance frameworks, which means that national and Union-level actors now face the challenge of reconciling rapid operational advances with the need for legal certainty,

procedural fairness and ex ante safeguards, and the most recent policy cycles have therefore seen a renewed emphasis on the role of data protection authorities, the codification of internal review procedures, and the clarification of parliamentary and judicial oversight, all of which are now viewed as essential for balancing anticipatory security with the preservation of rights and the maintenance of democratic accountability (Shepherd, 2024), (European Commission, 2020a). Interviews with practitioners and regulatory officials underline that even the best resourced agencies must now invest heavily in compliance infrastructure, training and transparency tools, since the expectation of the European public is not merely that security measures will be effective, but that they will be continuously justified, open to contestation, and ultimately reversible in the face of error or abuse (European Union Agency for Fundamental Rights, 2023), (Council of the European Union, 2022).

Consequently, the findings of this study suggest that the ongoing negotiation between operational effectiveness and rights protection has matured into a dynamic in which judicial, regulatory and societal actors regularly intervene to set new thresholds, to scrutinise both the logic and the impact of technical interventions, and to demand that every extension of state power be balanced by meaningful oversight, public debate and a commitment to transparency that is not merely rhetorical but is embedded in the daily routines of all actors involved in the security chain (Martinico & Dembinski, 2021), (Bures, 2016). In conclusion, while the European Union has achieved notable progress in mainstreaming rights protection and democratic legitimacy within its counterterrorism architecture, the challenge remains open-ended, as future advances in surveillance, analytics or crisis management will almost certainly provoke fresh rounds of legal, political and ethical reflection, and the ability of the Union to sustain its unique model of security will depend not only on technological prowess or legislative agility, but above all on the maintenance of public trust, the resilience of oversight structures and the deepening of a rights-based culture that can accommodate change without sacrificing its constitutional soul.

5.3 Institutional Gaps and Implementation Challenges

The comparative examination of institutional gaps and implementation challenges in the evolving architecture of European counterterrorism policy from 2015 to 2025 reveals a complex field in which supranational regulatory ambitions, divergent national legal traditions, and everyday operational contingencies continuously intersect, and this section seeks to synthesise the principal findings of the empirical investigation while identifying those persistent bottlenecks that must be addressed to sustain both policy effectiveness and

democratic legitimacy as the Union's security project matures (Bures, 2016). To begin, the evidence demonstrates that the Union's prioritisation of interoperability through large-scale information systems, particularly the expansion of the Schengen Information System and the embedding of the Passenger Name Record directive, has substantially increased the technical capacity of Member States to share intelligence, track suspicious movements, and coordinate alerts in near real time, yet the deployment of these infrastructures has been consistently hindered by legacy IT environments, skills gaps among operational staff, and variable fiscal commitments, so that the achievement of formal compliance milestones has rarely translated into uniformly high levels of integration or operational reliability across all jurisdictions (European Court of Auditors, 2022), (Czaplicki, 2021).

The French experience, as highlighted in interviews and secondary reporting, suggests that sustained political attention, regular budget appropriations, and mature administrative coordination can compress implementation timelines and ensure the practical alignment of national and European platforms, although case studies also reveal that localised bottlenecks and staff turnover occasionally disrupt the otherwise smooth operation of national nodes, particularly in periods of heightened threat when demand for system throughput increases sharply. By contrast, the German federation, despite benefiting from strong technical investment and the expertise of federal agencies, is repeatedly confronted with the challenge of mediating between national and regional authorities, and this inter-institutional negotiation, while valuable for preserving local accountability and adaptive problem-solving, can introduce delays, fragmented reporting chains, and occasional duplication of effort, as regional bodies prioritise their own risk assessments or interpretation of compliance guidance (Hartmann, 2022). The Greek case, which has evolved against a background of chronic resource constraints and competing administrative priorities, illustrates that external support from Union agencies and targeted co-financing can enable the upgrading of national systems to baseline standards, yet significant disparities remain between metropolitan and peripheral jurisdictions, so that island hotspots, border crossings, and overstretched police departments often lag behind urban centres in their ability to generate, process, and respond to shared alerts (Gkouvas & Kousoulis, 2021).

At the same time, the increasing reliance on Europol's analytical hubs and joint investigation platforms has facilitated the cross-border tracking of threat actors and the pooling of intelligence, and interviews with national liaison officers confirm that these institutional resources are now valued as much for their capacity to support long-term strategic foresight as for their role in short-term data enrichment, although persistent concerns remain about the

ability of shared analytical platforms to manage large and heterogeneous datasets without breaching data minimisation principles or provoking resistance from national data protection authorities, especially when the scope of data queries is expanded for preventive purposes (European Union Agency for Fundamental Rights, 2023), (eu-LISA, 2023). The practical integration of these platforms is further complicated by divergent national standards for data entry, access rights, and audit trails, meaning that operational momentum is sometimes lost in the process of harmonising procedural codes, translating technical schemas, or negotiating rules of evidence across administrative borders.

A further broad challenge arises from the translation of supranational legal innovation into durable organisational routines, because ministries and agencies tasked with implementing new directives or protocols must not only revise compliance manuals, train staff, and upgrade hardware, but also embed a culture of transparency, accountability, and proactive engagement with oversight authorities, and this process of organisational learning is frequently disrupted by shifts in political leadership, turnover among key personnel, or exogenous shocks such as major attacks or financial crises that divert attention from medium-term reform (Martinico & Dembinski, 2021). The evidence gathered for this research suggests that, while legislative transposition can be achieved within the timelines mandated by Union institutions, the embedding of new standards into daily practice depends heavily on leadership continuity, the existence of clear reporting lines, and the ability to maintain institutional memory even as recruitment, retirement, and intra-agency transfers alter the composition of operational teams (Tsakalidis & Tsiavos, 2020).

Moreover, it is clear that the interface between national and Union-level obligations remains a persistent source of tension, particularly where requirements for data protection, judicial authorisation, and the safeguarding of fundamental rights are interpreted differently by local courts, administrative tribunals, or independent oversight bodies, and here the jurisprudence of the Court of Justice of the European Union has established a set of substantive benchmarks regarding necessity, proportionality, and the minimisation of intrusive practices, but the actual translation of these norms into coherent administrative routines continues to depend on the resources, interpretive traditions, and risk appetites of national authorities, so that harmonisation remains a moving target rather than a completed process (Court of Justice of the European Union, 2022), (Papakonstantinou & Karyda, 2019). Comparative fieldwork further confirms that, in Germany, high levels of formal compliance coexist with the recurring challenge of mediating between regional and national priorities, while in France, centralised data protection authorities can respond quickly to emergent risks but sometimes

encounter resistance from decentralised operational units, and in Greece, limited staffing and resource differentials across administrative regions produce an uneven landscape of compliance and readiness that external monitoring alone cannot fully address (Hartmann, 2022), (Gkouvas & Kousoulis, 2021).

Interviews and institutional self-assessments also underline that the pace of technological innovation frequently outstrips the development of ethical, procedural, and cultural safeguards, so that artificial intelligence, predictive analytics, and automated screening tools are integrated into investigative routines before the required oversight structures, redress mechanisms, and quality controls are fully developed, creating new vulnerabilities not only for individual rights but also for the legitimacy and resilience of the entire security apparatus, especially when errors or biases go undetected or uncorrected (Shepherd, 2024), (European Union Agency for Fundamental Rights, 2023).

In conclusion, the accumulated evidence demonstrates that the next phase of the European Union's counterterrorism project must give priority not merely to the further expansion of technical systems or the refinement of legal texts, but to the deepening of institutional capacities, the cultivation of cooperative routines, and the consolidation of a rights-based culture of practice, where transparency, learning, and adaptability are recognised as essential attributes of resilience, and where every Member State, regardless of its starting conditions, is able to participate in and contribute to a collective security framework that is both operationally effective and democratically legitimate (Bures, 2016), (Martinico & Dembinski, 2021).

5.4 Strategic Balance between Security and Liberty

The comparative assessment of European counterterrorism policy from 2015 to 2025 highlights that the pursuit of a strategic balance between security and liberty stands at the heart of the Union's evolving security architecture, and this section attempts to bring together the principal empirical and normative insights that frame this dilemma, while tracing the institutional mechanisms and policy adjustments through which the Union and its Member States have sought to recalibrate the boundaries between collective safety and individual rights in response to changing threat environments and societal expectations (Bures, 2016). To begin, the last decade has witnessed an unprecedented expansion of legislative, technical and operational capacity, as the rollout of large-scale information systems, the harmonisation of cross-border investigative powers and the adoption of risk-based screening mechanisms have considerably enhanced the ability of authorities to detect, prevent and respond to threats

in real time, although the very success of these initiatives has repeatedly provoked renewed debate about proportionality, transparency and the permissible limits of state intervention in the lives of citizens (Directive (EU) 2016/681, 2016), (Czaplicki, 2021).

The French experience underscores that the acceleration of security reforms, driven by political urgency and a series of high-profile terrorist attacks, enabled rapid adoption of new surveillance measures and an expanded operational mandate for law enforcement agencies, yet public controversies over the breadth of emergency powers and the management of protest movements have revealed the potential for tension whenever executive prerogatives appear to encroach on freedom of assembly or the right to privacy, and similar dynamics can be observed in Germany, where strong legal and institutional safeguards have often acted as a counterweight to the expansion of risk-driven policing, leading to robust parliamentary debate and periodic judicial review that has on several occasions reshaped the contours of preventive detention, bulk data retention and the use of algorithmic risk profiling (Hartmann, 2022), (Court of Justice of the European Union, 2022). The Greek case, although marked by more limited resources and a distinct legal tradition, demonstrates that European funding and external guidance can facilitate the adoption of new security infrastructures, but the unevenness of implementation and the vulnerability of local oversight mechanisms sometimes expose the tension between the aspiration to harmonise security practice and the realities of institutional fragility or public scepticism (Gkouvas & Kousoulis, 2021), (Tsakalidis & Tsiavos, 2020).

At the same time, the Union-level regulatory process has played a pivotal role in clarifying and sometimes recalibrating the strategic balance, as the jurisprudence of the Court of Justice of the European Union has set substantive benchmarks for necessity and proportionality, insisting that measures which intrude on privacy, liberty or data protection be narrowly tailored, time-limited and subject to meaningful avenues of legal redress, and this judicial guidance has compelled both Union institutions and national legislatures to codify more rigorous standards for authorisation, oversight and the minimisation of intrusive practices (Court of Justice of the European Union, 2022), (Papakonstantinou & Karyda, 2019). Policy analysis further demonstrates that the evolution of security practice is not a linear process, but rather a dynamic negotiation in which technological innovation, political contingency and normative contestation intersect, so that new surveillance tools or data-sharing mandates are frequently revised, circumscribed or suspended in the wake of public challenge, judicial intervention or parliamentary inquiry, and the experience of Member States suggests that the durability of any strategic balance depends as much on the resilience of democratic oversight

and public trust as on the formal specification of rights and duties in legal text (European Union Agency for Fundamental Rights, 2023), (Martinico & Dembinski, 2021).

Moreover, the last decade has seen the rise of a more participatory model of governance, wherein civil society actors, data protection authorities and independent regulators are increasingly integrated into the design, review and monitoring of security policy, and the comparative evidence confirms that those national systems which most consistently engage a plurality of voices in the calibration of preventive measures are best able to anticipate and resolve emerging conflicts between security objectives and fundamental freedoms, thereby sustaining legitimacy and reducing the risk of marginalisation or societal backlash (European Commission, 2021), (Radicalisation Awareness Network, 2022). The French and German experiences reveal that while legal sophistication and institutional capacity are essential, the legitimacy of security policy ultimately rests on continuous public engagement, transparency and the demonstrable capacity of oversight bodies to hold executive agencies to account, and the Greek case highlights that even in the context of resource constraints, robust consultation and effective communication can mitigate public anxiety and foster a more inclusive, resilient approach to the security-liberty nexus (Gkouvas & Kousoulis, 2021), (Hartmann, 2022).

A further layer of complexity is introduced by the rapid pace of technological innovation, as the deployment of artificial intelligence, biometric identification and cross-referenced databases introduces both new opportunities for risk anticipation and new risks for rights protection, so that the challenge facing the Union is not only to update legal frameworks in line with technical possibilities, but also to ensure that the ethos of necessity, proportionality and democratic control is continually renewed as practices evolve and as new societal expectations are articulated (Shepherd, 2024), (European Union Agency for Fundamental Rights, 2023). Fieldwork and institutional reviews underline that the strategic balance between security and liberty is sustained not through the static allocation of rights and powers, but through an ongoing process of negotiation, adaptation and critical self-assessment, in which executive agencies, judicial authorities, oversight bodies and the public itself are continuously engaged in reassessing the boundaries of permissible intervention and in updating the institutional routines that safeguard both collective safety and individual autonomy (Martinico & Dembinski, 2021), (Bures, 2016).

In summary, the evidence confirms that the strategic balance between security and liberty in the European Union is neither a matter of technical optimisation nor a one-time constitutional settlement, but rather a living project that requires the continuous renewal of democratic institutions, the deepening of public dialogue and the embedding of rights-based safeguards

within the everyday routines of governance, and the capacity of the Union and its Member States to sustain this equilibrium will remain a critical test of the resilience, legitimacy and future direction of the European security project (Martinico & Dembinski, 2021), (Bures, 2016).

5.5 Critical Review of Existing Policies and Programmes

The critical review of existing policies and programmes in the domain of European counterterrorism from 2015 to 2025 reveals a policy environment defined by overlapping layers of supranational regulation, national adaptation, and practical experimentation, and this section attempts to draw together the principal findings of the empirical research in order to assess the effectiveness, sustainability and long-term coherence of the Union's most significant legislative, technical and operational interventions (Bures, 2016). To begin, it is evident that the drive for greater interoperability and information sharing has animated the bulk of the policy innovation over the last decade, as the adoption of successive regulations on the Schengen Information System, the Passenger Name Record directive and the rollout of the Entry/Exit System have together created a technical infrastructure capable of supporting real-time cross-border tracking, risk assessment and joint investigative operations, yet fieldwork and audit reports indicate that the practical impact of these tools has been shaped as much by the unevenness of national infrastructure, legal harmonisation and administrative capacity as by the ambition of the regulatory texts themselves (European Court of Auditors, 2022), (Czaplicki, 2021).

The French and German cases provide instructive contrasts, because France has been able to leverage a tradition of administrative centralisation and strong fiscal support to achieve rapid integration of new platforms, thereby increasing the speed and reliability of alerts and the accessibility of biometric and travel data for operational teams, while the German federation, with its dense network of regional authorities and decentralised security architecture, has frequently encountered challenges in harmonising data standards, aligning investigative protocols and ensuring the consistency of risk assessments across federal and Land-level agencies, which in practice means that the effectiveness of Union-level systems is frequently modulated by local priorities and resource allocations (Hartmann, 2022). The Greek experience, as highlighted by both national evaluations and Union monitoring, shows that targeted funding and technical assistance can enable baseline compliance even in resource-constrained environments, although significant implementation gaps persist in peripheral jurisdictions, particularly in island and border areas where staff turnover, infrastructure

limitations and overlapping mandates can impede the flow of information and the reliability of alerts (Gkouvas & Kousoulis, 2021), (Tsakalidis & Tsiavos, 2020).

A second broad theme concerns the regulatory and normative architecture of prevention and prosecution, since instruments such as Directive (EU) 2017/541 on combating terrorism and the European Union's counter-radicalisation strategies have expanded the legal bases for anticipatory interventions, cross-border investigations and the criminalisation of preparatory acts, but have also generated debate about the necessity, proportionality and human rights compliance of measures such as pre-emptive detention, online content removal and algorithmic risk scoring (Directive (EU) 2016/681, 2016), (Papakonstantinou & Karyda, 2019). The empirical record indicates that while these measures have increased the technical and legal capacity of authorities to disrupt attack planning and monitor emergent threats, they have also produced new challenges for judicial review, data protection and democratic oversight, as courts in Paris, Karlsruhe and Athens have on several occasions invoked constitutional and Union law principles to circumscribe, revise or even annul measures deemed insufficiently justified or inadequately constrained by procedural safeguards (Court of Justice of the European Union, 2022), (Tsiftsoglou, 2022).

Moreover, the role of Europol and the European Counter Terrorism Centre has grown steadily, with Member States increasingly relying on shared analytical platforms, joint investigation teams and the pooling of criminal intelligence to identify cross-border threat patterns, yet interviews with practitioners and policy analysts confirm that the integration of these platforms into national workflows remains incomplete, due to disparities in data quality, the timeliness of contributions and lingering mistrust or uncertainty about the sharing of sensitive operational information (European Union Agency for Fundamental Rights, 2023), (eu-LISA, 2023). The French and German experiences suggest that sustained investment in analytical capacity and the cultivation of trusted liaison relationships can yield operational dividends, but the Greek case demonstrates that the value of supranational support is closely tied to the existence of local capacity and the clarity of procedural guidance, since under-resourced agencies can find themselves overwhelmed by the demands of new reporting protocols or the management of complex, multi-agency investigations (Gkouvas & Kousoulis, 2021).

A further aspect of the critical review concerns the long-term sustainability and adaptability of the Union's counterterrorism architecture, because although the proliferation of technical systems and the expansion of legal mandates have enabled rapid responses to evolving threats, the evidence indicates that the durability and resilience of these advances are

contingent on the capacity of institutions to absorb new practices, adapt to shifting political priorities and maintain institutional memory in the face of staff turnover and external shocks (Martinico & Dembinski, 2021), (Bures, 2016). Comparative analysis demonstrates that those jurisdictions which invest consistently in training, review and the embedding of oversight structures are better able to sustain the gains achieved through regulatory innovation, while those that treat policy adoption as a one-time event or fail to cultivate a culture of compliance, learning and adaptation risk seeing the effectiveness of new measures eroded over time.

In conclusion, the critical review of existing policies and programmes underscores that while the European Union has achieved substantial progress in building a multi-layered, technically sophisticated and legally harmonised counterterrorism framework, significant challenges remain in translating formal compliance into effective practice, in maintaining a principled balance between security and rights, and in ensuring that national and supranational systems evolve together in response to new threats and societal expectations, so that the legitimacy, effectiveness and resilience of European counterterrorism policy will ultimately depend on the Union's ability to foster continuous learning, transparent evaluation and adaptive governance across all levels of the security architecture (Martinico & Dembinski, 2021), (European Union Agency for Fundamental Rights, 2023).

Chapter 6: Conclusions and Policy Recommendations

6.1 Recapitulation of Key Findings

The recapitulation of key findings from this study, which has examined the evolution of European counterterrorism policy from 2015 to 2025 through a comparative and multi-level lens, reveals a security landscape whose complexity is matched only by the persistence of unresolved tensions between the demands of effective prevention, the imperatives of democratic legitimacy and the practical realities of institutional adaptation, and this section aims to synthesise the main empirical and analytical insights that have emerged across the preceding chapters while drawing out the core lessons for future policy and research (Bures, 2016). To begin, the evidence demonstrates that the European Union's effort to construct an integrated security architecture, grounded in the proliferation of large-scale information systems and the harmonisation of legal frameworks, has yielded substantial gains in terms of technical capacity, cross-border interoperability and the speed with which authorities can detect, assess and respond to emergent threats, yet the process of embedding these innovations in the daily routines of national administrations has exposed persistent gaps in infrastructure, skills and the mutual alignment of procedural standards, so that headline progress at the Union level has often masked enduring discrepancies in the effectiveness and reliability of local implementation (European Court of Auditors, 2022), (Czaplicki, 2021).

The comparative analysis of France, Germany and Greece illustrates that while the former two have been able to leverage longstanding institutional strengths, sustained fiscal investment and traditions of administrative coordination to accelerate the adoption of new platforms and procedures, their experiences nevertheless reveal ongoing challenges in harmonising the practices of regional and central authorities, ensuring the reliability of data flows and maintaining high levels of compliance across complex, multi-level governance structures, and the Greek case, meanwhile, highlights the crucial role of external support, targeted co-financing and intensive training in enabling resource-constrained administrations to achieve baseline compliance, although persistent disparities between metropolitan and peripheral regions, as well as the legacy of fiscal austerity, continue to limit the reach and sustainability of these advances (Hartmann, 2022), (Gkouvas & Kousoulis, 2021).

A further central finding concerns the dynamic interplay between technological innovation and rights protection, because while the deployment of artificial intelligence, predictive analytics and biometric identification has undeniably expanded the capacity of authorities to

anticipate, profile and disrupt risk, these same innovations have provoked intense debate and, at times, legal contestation regarding the necessity, proportionality and accountability of preventive measures, with the jurisprudence of the Court of Justice of the European Union and the oversight of national data protection authorities together ensuring that the operational reach of surveillance technologies is continuously recalibrated in line with evolving standards of fundamental rights, judicial review and public transparency (Court of Justice of the European Union, 2022), (Shepherd, 2024). Empirical research confirms that the durability and legitimacy of counterterrorism policy now depends as much on the credibility of oversight routines, the accessibility of redress mechanisms and the meaningful involvement of civil society in both design and review as on the formal sophistication of legal or technical instruments, since the resilience of the security architecture is ultimately determined by its capacity to command societal trust and to adapt responsively to new challenges and critiques (European Union Agency for Fundamental Rights, 2023), (Papakonstantinou & Karyda, 2019).

At the same time, the analysis demonstrates that the effectiveness and legitimacy of Union-level policies are shaped not only by legal harmonisation and technical interoperability but also by the institutional memory, leadership continuity and learning culture of national and supranational agencies, with those administrations that invest consistently in training, monitoring and review able to sustain policy gains over time, while those that neglect these elements risk seeing the practical value of new frameworks eroded by staff turnover, shifting political priorities or external shocks (Martinico & Dembinski, 2021), (Tsakalidis & Tsiavos, 2020). The integration of community engagement, youth-focused prevention and local dialogue initiatives into the mainstream of counterterrorism strategy further underscores the move toward a more participatory and holistic approach, one in which resilience is understood as a function not only of technological and legal assets but also of social cohesion, trust-building and the ability of institutions to listen, adapt and respond to diverse needs and concerns (European Commission, 2021), (Radicalisation Awareness Network, 2022).

In conclusion, the key findings of this research underscore that while the European Union has made remarkable progress in building a more interconnected, technically advanced and rights-conscious counterterrorism system, the ongoing challenges of institutional diversity, rights protection and adaptive governance demand a sustained commitment to continuous learning, critical self-assessment and the cultivation of a security culture that is both operationally robust and democratically legitimate, so that the promise of European security

is realised not only in headline achievements but in the everyday practices and lived experience of all those subject to its rules (Bures, 2016), (Martinico & Dembinski, 2021).

6.2 Addressing the Research Questions

The systematic addressing of the research questions guiding this inquiry into European counterterrorism policy from 2015 to 2025 provides an opportunity not only to synthesise the empirical findings and theoretical reflections of the preceding chapters, but also to demonstrate how the interplay of supranational regulatory ambition, national legal adaptation, and practical operational realities has shaped both the effectiveness and the legitimacy of the Union's evolving security architecture (Bures, 2016). To begin, the central question concerning the extent to which supranational initiatives have succeeded in fostering genuine interoperability and technical integration across Member States can be answered by reference to the documented rollout of large-scale information systems such as the second-generation Schengen Information System and the Passenger Name Record framework, since these platforms have enabled unprecedented cross-border sharing of alerts, biometric identifiers, and travel histories, thereby advancing the technical capacity of authorities to monitor and respond to emergent threats in real time, although the practical value of these innovations has been tempered by persistent discrepancies in national infrastructure, staff training, and the ability of local agencies to align with evolving Union standards (European Court of Auditors, 2022), (Czaplicki, 2021).

The comparative evidence drawn from France, Germany, and Greece further elucidates the unevenness of policy implementation and operational effectiveness, as France's tradition of administrative centralisation and fiscal support facilitated rapid adaptation, Germany's complex federal structure introduced coordination challenges between regional and central authorities, and Greece's resource-constrained context revealed both the enabling role of Union co-financing and the persistent risk of implementation gaps in peripheral or high-pressure jurisdictions, thus confirming that formal compliance at the legislative level does not always ensure uniform performance in daily practice (Hartmann, 2022), (Gkouvas & Kousoulis, 2021). A second key research question focused on the ways in which the expansion of preventive policing powers and the adoption of advanced surveillance technologies have affected the balance between security and fundamental rights, and the findings indicate that, while technical sophistication and legal harmonisation have strengthened the capacity to pre-empt and disrupt risk, they have simultaneously generated new sites of contestation, as judicial authorities, regulatory bodies, and civil society actors

have repeatedly intervened to challenge, revise, or recalibrate those measures deemed excessive, insufficiently transparent, or at risk of undermining the principles of necessity and proportionality (Court of Justice of the European Union, 2022), (Papakonstantinou & Karyda, 2019).

The jurisprudence of the Court of Justice of the European Union, as well as national constitutional courts, has played a pivotal role in enforcing substantive safeguards, insisting on the continual reassessment of risk modelling, the minimisation of data retention, and the availability of effective remedies for those affected by intrusive interventions, and this ongoing judicial and regulatory engagement has helped to embed a culture of rights-consciousness and accountability within the evolving security framework, even as technological innovation, political urgency, and societal expectations continue to drive policy reform (Tsiftsoglou, 2022), (Shepherd, 2024). A third research question considered the extent to which participatory governance and community engagement have become integrated into mainstream policy, and the evidence confirms a gradual shift toward more inclusive models of prevention, as initiatives designed to foster local dialogue, empower youth, and strengthen grassroots resilience have been increasingly incorporated into national and Union-level strategies, thus reinforcing the understanding that sustainable security is built not only on technical and legal assets but also on social trust, communication, and the credibility of oversight mechanisms (European Commission, 2021), (Radicalisation Awareness Network, 2022).

Finally, the analysis confirms that the ability of the European Union and its Member States to sustain policy gains, adapt to shifting threat landscapes, and maintain democratic legitimacy is closely tied to the quality of institutional memory, the continuity of leadership, and the willingness to invest in ongoing training, evaluation, and the meaningful engagement of all relevant stakeholders, so that the challenges of institutional diversity, rights protection, and adaptive governance are addressed not through static compliance but through a dynamic process of learning, dialogue, and reflexive policy adjustment (Martinico & Dembinski, 2021), (Bures, 2016). In summary, the research questions that animated this study have been addressed through a combination of empirical case analysis, theoretical synthesis, and critical reflection, highlighting both the achievements and the continuing challenges that define the European counterterrorism project at the close of the current decade.

6.3 Policy Recommendations for the European Union

The policy recommendations that arise from the comparative analysis of European counterterrorism from 2015 to 2025 are grounded in the recognition that the evolving security architecture of the Union has achieved significant progress in enhancing technical interoperability, legislative harmonisation and cross-border operational capacity, yet continues to be challenged by persistent discrepancies in institutional capability, resource allocation, rights protection and the practical embedding of democratic legitimacy, and this section aims to synthesise the principal lessons of the empirical and analytical chapters in order to offer concrete, evidence-based proposals for the further development and consolidation of a resilient, effective and principled security framework (Bures, 2016). To begin, it is recommended that the European Union prioritise sustained investment in the upgrading of national infrastructure and the professional development of operational staff, since the evidence demonstrates that the technical sophistication of information systems such as the Schengen Information System, the Passenger Name Record architecture and the Entry/Exit System is only fully realised where Member States can guarantee the reliability, timeliness and quality of data flows, and the comparative experience of France, Germany and Greece underlines that both centralised and federalised systems require continuous training, regular review of protocols and targeted funding for resource-constrained regions in order to overcome legacy bottlenecks, staff turnover and uneven adaptation to supranational standards (European Court of Auditors, 2022), (Czaplicki, 2021).

A second core recommendation is that Union institutions and national governments reinforce the structures and routines of democratic oversight, judicial review and independent monitoring, as the proliferation of advanced surveillance technologies, algorithmic risk assessment tools and predictive policing models brings with it not only opportunities for anticipatory threat management but also new risks of overreach, error and public distrust, so that the legitimacy and sustainability of preventive measures will depend on the regular engagement of data protection authorities, parliamentary committees, civil society organisations and independent regulators in the ongoing design, implementation and evaluation of security interventions (Court of Justice of the European Union, 2022), (Papakonstantinou & Karyda, 2019). The jurisprudence of the Court of Justice of the European Union and the comparative experience of Member States confirm that the embedding of robust safeguards for necessity, proportionality, transparency and redress is indispensable, and the Union should therefore support the standardisation of audit trails, the

routine publication of impact assessments and the development of accessible channels for complaints, review and the correction of error or abuse, while also fostering a culture of openness and critical reflection within executive agencies (Tsiftsoglou, 2022), (European Union Agency for Fundamental Rights, 2023).

A further key recommendation is to advance the integration of participatory governance and local engagement into the core of counterterrorism strategy, because the resilience and legitimacy of the Union's security architecture is not only a function of technical prowess or legislative precision, but equally a product of societal trust, community partnership and the credibility of dialogue between authorities and the populations most directly affected by preventive measures (European Commission, 2021), (Radicalisation Awareness Network, 2022). The comparative review of national cases demonstrates that the most sustainable and context-sensitive outcomes have emerged in those jurisdictions where governments have invested in youth-oriented prevention, intercultural dialogue, and the early involvement of grassroots actors, and the Union should therefore support Member States in the scaling-up of local initiatives, the sharing of best practices, and the development of metrics and evaluation frameworks that can capture both operational results and social impact, thereby ensuring that preventive policy is rooted in an ongoing process of consultation, feedback and adaptive learning (Gkouvas & Kousoulis, 2021), (Hartmann, 2022).

Moreover, it is recommended that the Union reinforce the capacity for adaptive governance and institutional learning, as the pace of technological innovation, the shifting nature of threat landscapes and the volatility of political cycles demand that both Union and national agencies cultivate organisational cultures capable of anticipating new risks, evaluating unintended consequences and integrating new knowledge into everyday routines, so that the security framework can remain both robust and flexible in the face of emerging challenges (Martinico & Dembinski, 2021), (Bures, 2016). To this end, investments in training, cross-agency secondments, scenario-based exercises and collaborative platforms should be expanded, while the Union should also facilitate peer learning, independent research and the comparative assessment of national experiences in order to accelerate the diffusion of innovation and the identification of persistent gaps or bottlenecks (eu-LISA, 2023).

Finally, the Union should ensure that all future policy development is guided by a principled commitment to the protection of fundamental rights and the maintenance of democratic legitimacy, as the evidence confirms that only those security interventions that are firmly anchored in respect for the rule of law, the minimisation of intrusion and the cultivation of public trust can achieve durable effectiveness and societal acceptance (European Union

Agency for Fundamental Rights, 2023), (Council of the European Union, 2022). In practice, this means that legislative initiatives should be preceded by meaningful impact assessments, the use of artificial intelligence and big data analytics should be subject to clear legal boundaries and oversight, and every operational expansion should be accompanied by safeguards for transparency, equity and redress, so that the European security project remains true to its foundational values while adapting dynamically to new risks and opportunities (Shepherd, 2024), (Martinico & Dembinski, 2021).

In summary, the recommendations advanced in this section emphasise the need for sustained investment in capacity building, the deepening of democratic and societal oversight, the integration of local partnership and participatory governance, the cultivation of adaptive institutional cultures and the rigorous protection of rights, so that the European Union's counterterrorism architecture can continue to evolve in ways that are both operationally effective and normatively legitimate, capable of responding to changing threats without sacrificing the values that have long distinguished the European project (Bures, 2016), (Martinico & Dembinski, 2021).

6.4 Proposed Institutional and Legislative Reforms

The formulation of proposed institutional and legislative reforms for the European Union's counterterrorism framework is rooted in the recognition that, while significant progress has been achieved in establishing a robust architecture for information sharing, operational cooperation, and legal harmonisation, persistent disparities in institutional capacity, procedural standards, and rights protection continue to constrain the full realisation of policy objectives, and this section sets out targeted recommendations that build on empirical findings and comparative analysis in order to enhance the effectiveness, resilience, and legitimacy of the Union's security project (Bures, 2016). To begin, it is recommended that the Union and its Member States move beyond ad hoc system upgrades and pursue a strategy of long-term institutional consolidation, focusing on regular investments in workforce training, infrastructure modernisation, and the embedding of new legal instruments within stable administrative routines, since the evidence from France, Germany, and Greece demonstrates that sustainable adaptation depends as much on the cultivation of professional cultures of transparency and accountability as on the technical sophistication of the underlying systems (European Court of Auditors, 2022), (Czaplicki, 2021).

A second reform priority concerns the reinforcement of cross-border cooperation mechanisms, as the effectiveness of large-scale information systems and joint operational

platforms is heavily shaped by the ability of national agencies to interpret, validate, and act upon shared alerts in real time, and the comparative experience reveals that operational bottlenecks frequently arise not only from technical incompatibilities but also from the absence of standardised procedures, joint training opportunities, and institutionalised channels for mutual assistance and knowledge transfer (Hartmann, 2022), (eu-LISA, 2023). The Union should therefore invest in the development of common training curricula, multilingual procedural guidance, and secondment programmes, enabling operational staff to build the trust and analytical capacity required for rapid and reliable cooperation, particularly in regions that have historically struggled with resource limitations or high turnover among key personnel (Gkouvas & Kousoulis, 2021).

At the legislative level, the Union should institutionalise a process of regular review and, where needed, timely revision of foundational directives and regulations, so that evolving threat environments, technological capabilities, and jurisprudential developments are systematically reflected in the legal framework, and this should include the structured evaluation of the practical impact of Directive (EU) 2017/541 and the main interoperability regulations, drawing on the perspectives of practitioners, oversight bodies, and affected communities to ensure that regulatory adjustments are both empirically grounded and rights-sensitive (Papakonstantinou & Karyda, 2019), (Tsiftsoglou, 2022). Such a framework would enable the early identification of implementation gaps, procedural loopholes, or emerging rights risks, and facilitate responsive adaptation in line with evolving jurisprudence from both the Court of Justice of the European Union and national courts (Court of Justice of the European Union, 2022), (European Union Agency for Fundamental Rights, 2023).

Moreover, it is essential to intensify efforts to mainstream data protection and ethical oversight into all stages of policy and operational development, as the growing use of artificial intelligence, algorithmic risk assessment, and predictive analytics introduces new challenges for accountability, bias mitigation, and public trust, and the Union should support the establishment of clear audit criteria, independent review mechanisms, and the integration of ethical impact assessments into the legislative process (Shepherd, 2024), (European Union Agency for Fundamental Rights, 2023).

In conclusion, the proposed institutional and legislative reforms outlined here are intended to reinforce the adaptability, resilience, and legitimacy of the European Union’s counterterrorism framework, ensuring that the Union remains able to anticipate and respond to evolving threats while maintaining a principled commitment to rights protection, democratic accountability, and inclusive governance (Martinico & Dembinski, 2021), (Bures,

2016).

6.5 Limitations of the Study and Directions for Future Research

A careful consideration of the study's limitations is essential for contextualising the scope and implications of its findings, since the process of conducting a comparative analysis of European counterterrorism policy across France, Germany and Greece has been continuously shaped by unavoidable constraints relating to case selection, data availability, and the shifting nature of the security landscape, and the first and perhaps most evident limitation concerns the fact that the selection of three Member States, while permitting a nuanced and empirically grounded exploration of administrative variety and policy outcomes, necessarily precludes the incorporation of alternative national contexts whose institutional architectures, socio-political environments or levels of threat exposure might generate divergent patterns or even unanticipated exceptions to the trends documented in this research (Bures, 2016). Although the rationale for focusing on these particular cases was based on their representative contrasts in terms of governance capacity, resource allocation and legal tradition, the possibility remains that additional Member States, especially those with different historical experiences or forms of civil-military coordination, would reveal further dynamics that could either reinforce or complicate the conclusions drawn here (Hartmann, 2022).

Furthermore, the empirical investigation has been shaped by differences in institutional transparency, the public availability of data and the reliability of official reporting, as some jurisdictions maintain more comprehensive records, offer greater access to audit documentation or support deeper engagement with external researchers, while others impose restrictions for reasons of confidentiality, operational secrecy or the protection of sensitive information, which inevitably results in asymmetries in the depth and granularity of the comparative evidence (European Court of Auditors, 2022), (Gkouvas & Kousoulis, 2021). While the combination of official documents, secondary data and expert interviews has provided a robust foundation for empirical triangulation, it must be acknowledged that certain aspects of day-to-day practice, informal negotiation or micro-level adaptation have had to be inferred indirectly, and that the lived experience of communities subject to preventive measures or of frontline practitioners may not always be fully captured through available sources (Papakonstantinou & Karyda, 2019).

In addition, the evolving and sometimes unpredictable nature of both the policy field and the threat environment means that findings recorded during the period of research may be quickly overtaken by legislative amendments, institutional restructuring or the emergence of

new risk vectors, such as the rapid diffusion of artificial intelligence technologies, shifts in judicial interpretation or the cascading effects of external shocks, and while every effort has been made to integrate the most recent evidence and to follow the trajectory of major developments, the fast-moving pace of events in European security governance means that some relevant changes or innovations may not yet be reflected in the available data (Shepherd, 2024), (European Union Agency for Fundamental Rights, 2023). Moreover, the filtering of certain stakeholder perspectives through institutional gatekeepers, necessary for ethical and confidentiality reasons, may have inadvertently limited the representation of critical or dissenting voices, especially among marginalised groups or those whose experience with security interventions diverges from official accounts.

Looking forward, the limitations identified here suggest several promising directions for future research. One clear priority is the expansion of the comparative frame to include a wider array of Member States, with particular attention to those situated at the geographical or institutional periphery of the Union, as well as countries that have pioneered novel approaches to prevention, data governance or participatory oversight, since such studies could deepen understanding of the conditions under which specific institutional configurations or policy innovations are most likely to produce resilient, legitimate and effective outcomes (Tsakalidis & Tsiavos, 2020). Another avenue involves the adoption of longitudinal and ethnographic research designs capable of tracing the translation of policy into daily practice, uncovering the informal routines, learning dynamics and adaptive strategies through which new rules, technologies or participatory mechanisms are actually integrated into administrative cultures or recalibrated in response to local constraints (European Commission, 2021), (Radicalisation Awareness Network, 2022).

There is also an urgent need for interdisciplinary work at the intersection of law, technology and social science, especially in the context of artificial intelligence, algorithmic decision-making and predictive analytics, because the accelerating adoption of these tools raises complex questions about accountability, bias mitigation, explainability and the procedural safeguards required to maintain public trust and judicial legitimacy in rapidly evolving operational environments (Shepherd, 2024), (European Union Agency for Fundamental Rights, 2023). Finally, future research would benefit from a sustained focus on participatory governance, trust-building, and the mechanisms that facilitate the inclusion of diverse voices in both policy design and oversight, in order to move beyond formal consultation toward the empirical assessment of when and how such processes contribute to legitimacy, resilience and the early identification of unintended consequences (Martinico & Dembinski, 2021),

(Bures, 2016).

In summary, while the present study offers an empirically grounded and theoretically informed analysis of recent developments in European counterterrorism, the field remains marked by complexity, rapid evolution and the continuing need for critical, reflexive and context-sensitive scholarship that remains open to new evidence, methods and perspectives.

6.6 Final Reflections

The culmination of this comparative inquiry into European counterterrorism from 2015 to 2025 underscores that the project of safeguarding citizens while preserving democratic integrity remains an inherently dynamic and unfinished endeavour, since the evolution of legal frameworks, technical infrastructures and institutional cultures has been continuously shaped by shifting threat landscapes, societal expectations and normative constraints, and the preceding chapters have demonstrated that progress is best understood not as a linear trajectory toward a settled equilibrium, but as a series of iterative adjustments in which each advance is tested against emerging risks, legal scrutiny and public debate (Bures, 2016). One overarching insight concerns the extent to which the Union has succeeded in establishing a shared vocabulary and a set of procedural tools that permit authorities across diverse national settings to cooperate in real time, exchange sensitive information and coordinate investigative efforts, yet the practical value of these instruments remains conditioned by the political will, resource endowment and administrative readiness of individual Member States, so that the persistent variation in implementation continues to offer both challenges and opportunities for collective learning and adaptation (European Court of Auditors, 2022), (Czaplicki, 2021).

At the same time, the study has shown that the legitimacy of counterterrorism policy now rests as much on the transparency, accountability and inclusiveness of institutional processes as on the sheer technical prowess of surveillance tools or the formal precision of legislative texts, because public trust, judicial oversight and the credibility of independent regulators have emerged as indispensable pillars of a resilient security architecture, and the jurisprudence of the Court of Justice of the European Union, together with the monitoring of national data protection authorities, has played a central role in ensuring that each extension of preventive power is tempered by safeguards for necessity, proportionality and effective remedy, thereby embedding a rights conscious ethos within the operational routines of executive agencies (Court of Justice of the European Union, 2022), (European Union Agency for Fundamental Rights, 2023).

A further reflection relates to the transformative impact of technological innovation, since the

diffusion of artificial intelligence, biometric recognition and predictive analytics has significantly expanded the toolkit available for anticipatory threat management, yet has also accelerated the need for robust ethical governance, algorithmic transparency and interdisciplinary collaboration, reminding policymakers that technical sophistication must always be matched by legal clarity, procedural fairness and continuous critical evaluation if long term legitimacy is to be preserved (Shepherd, 2024). The comparative cases of France, Germany and Greece illustrate that the capacity to harness technological opportunities while mitigating risks depends on the alignment of strategic investment, professional training and participatory dialogue, with France leveraging centralised coordination for rapid deployment, Germany relying on layered oversight to refine applications and Greece demonstrating how targeted Union support can bridge capacity gaps even as uneven resource distribution continues to pose challenges for consistent practice across metropolitan and peripheral contexts (Hartmann, 2022), (Gkouvas & Kousoulis, 2021).

Looking forward, the research suggests that the durability of the European security project will hinge on an institutional culture that values reflexivity, inclusiveness and adaptive governance, since the threats confronting the Union are likely to remain fluid, transnational and technologically mediated, while societal tolerance for intrusive measures will continue to depend on the demonstrable commitment of authorities to uphold fundamental rights, engage diverse stakeholders and communicate the rationale, scope and safeguards of preventive interventions in clear and accessible language (European Commission, 2021), (Radicalisation Awareness Network, 2022). The policy recommendations advanced in the preceding section therefore emphasise sustained investment in capacity building, the strengthening of cross border cooperation routines, the institutionalisation of periodic legislative review and the mainstreaming of data protection and ethical oversight at every stage of policy development and operational practice, and these recommendations are grounded in the empirical finding that institutional resilience is created not only by technological innovation or legal harmonisation, but equally by the everyday practices of consultation, monitoring and corrective learning through which complex systems maintain their balance in the face of unforeseen pressures (Martinico & Dembinski, 2021), (Bures, 2016).

In conclusion, this study affirms that the European Union has made significant strides toward a security framework that is at once operationally robust and normatively grounded, yet also highlights that true resilience will depend on the Union’s willingness to embrace continuous self assessment, to invest in the capacities of all Member States and to deepen a culture of accountability that treats citizens not merely as objects of protection but as active partners in

shaping the parameters of collective safety and individual liberty.

References

Bakker, E. (2015). Terrorism and Counterterrorism Studies: 50 Key Issues. Leiden: Leiden University Press.

Balzacq, T. (2011). Securitization Theory: How Security Problems Emerge and Dissolve. London: Routledge.

Beck, U. (2006). Risk Society: Towards a New Modernity (2nd ed.). London: Sage.

Bouhana, N., & Wikström, P.-O. (2011). Al-Qaeda-Inspired Terrorism in the European Union. Stockholm: Swedish National Defence College.

Bures, O. (2016). EU Counter-Terrorism Policy: A Paper Tiger? (2nd ed.). London: Routledge.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner.

Court of Justice of the European Union (CJEU). (2022). Joined Cases C-793/19 & C-794/19 – Passenger Name Record (PNR) Data. Luxembourg: CJEU.

Coolsaet, R. (2016). Jihadi Terrorism in Europe: The IS Effect (Egmont Paper 92). Brussels: Royal Institute for International Relations.

Council of the European Union. (2022). A Strategic Compass for Security and Defence. Brussels: Council of the EU.

Crenshaw, M. (1981). The causes of terrorism. Comparative Politics, 13(4), 379–399.

Czaplicki, K. (2021). Schengen Information System (SIS): Principles and evolution. Geospatial Information Science, 24(2), 123–137.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Official Journal of the European Union, L 119, 4 May 2016.

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism. Official Journal of the European Union, L 88, 31 March 2017.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. Official Journal of the European Union, L 333, 27 December 2022.

European Commission. (2020a). EU Security Union Strategy 2020-2025 (COM(2020) 605

final). Brussels.
European Commission. (2020b). A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond (COM(2020) 795 final). Brussels.
European Commission. (2021). Preventing Radicalisation Leading to Violent Extremism: RAN Progress Report. Brussels.
European Commission. (2023). Communication on the Entry into Operation of the Renewed Schengen Information System (COM(2023) 135 final). Brussels.
European Commission. (2024). State of Play and Roadmap for the Entry/Exit System and ETIAS (COM(2024) 92 final). Brussels.
European Court of Auditors. (2022). Special Report 13/2022: The EU's Large-Scale IT Systems in the Area of Freedom, Security and Justice. Luxembourg.
European Data Protection Supervisor (EDPS). (2022). Decision on the Retention by Europol of Datasets Lacking Data-Subject Categorisation. Brussels: EDPS.
European Union Agency for Fundamental Rights (FRA). (2023). Fundamental Rights Report 2023. Vienna: FRA.
Europol. (2016). European Union Terrorism Situation and Trend Report 2016 (TE-SAT 2016). The Hague: Europol.
Europol. (2024). European Union Terrorism Situation and Trend Report 2024 (TE-SAT 2024). The Hague: Europol.
eu-LISA. (2023). Consolidated Annual Activity Report 2023. Tallinn: eu-LISA.
Gkouvas, A., & Kousoulis, A. (2021). Preventing radicalisation in Greek urban communities: The role of municipal social services. Journal of Deradicalization, 26, 52–78.
Gurr, T. R. (2006). Economic factors and the origins of terrorism. In B. M. Jenkins (Ed.), The Origins of Terrorism: Classic Readings (pp. 97–130). London: Routledge.
Hartmann, J. (2022). Implementation gaps in EU counterterrorism: A member-state comparison. Journal of Common Market Studies, 60(3), 521–540.
Howorth, J., & Gheciu, A. (2018). Security and defence policy in the European Union. In B. Tonra, T. Christiansen, & T. A. Börzel (Eds.), The Routledge Handbook of European Security (pp. 277–292). London: Routledge.
Machado, A., & Liesching, K. (2019). The Passenger Name Record directive and fundamental rights. European Law Journal, 25(4), 321–340.
Martinico, G., & Dembinski, P. L. (2021). Counter-terrorism and the EU's rule-of-law dilemma. Common Market Law Review, 58(5), 1481–1512.
Mitsilegas, V. (2018). EU Criminal Law after Lisbon: Rights, Trust and the Transformation

of Justice in Europe. Oxford: Hart Publishing.

Neumann, P. R. (2013). The trouble with radicalization. International Affairs, 89(4), 873–893.

Neumann, P. R. (2017). Countering Violent Extremism and Radicalisation That Lead to Terrorism: Ideas, Recommendations and Good Practices. The Hague: International Centre for Counter-Terrorism.

Papakonstantinou, V., & Karyda, M. (2019). Passenger Name Records and the Greek legal order: Proportionality and oversight concerns. Computer Law & Security Review, 35(4), 105324.

Radicalisation Awareness Network (RAN). (2022). Practitioners' Insights: Youth Engagement and Trust-Building in P/CVE. Brussels: European Commission.

Reed, A., Ingram, H., & Whittaker, J. (2019). Online Extremism and Terrorism Research Ethics. Dublin: VOX-Pol Network of Excellence.

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN). Official Journal of the European Union, L 135, 22 May 2019.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on interoperability between EU information systems in the field of borders and visa. Official Journal of the European Union, L 135, 22 May 2019.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on interoperability between EU information systems in police and judicial cooperation, asylum and migration. Official Journal of the European Union, L 135, 22 May 2019.

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. Official Journal of the European Union, L 172, 17 May 2021.

Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulations (EU) 2016/794 and 2018/1725 as regards Europol's cooperation with private parties, processing of personal data and support for research and innovation. Official Journal of the European Union, L 169, 27 June 2022.

Shepherd, M. N. F. (2024). The Radicalisation Potential of Artificial Intelligence (ICCT Policy Brief). The Hague: ICCT.

Tsakalidis, A., & Tsiavos, P. (2020). Cybersecurity capacity in Greece: Policy gaps and strategic challenges. Hellenic Review of European Affairs, 25(1), 23–38.

Tsiftsoglou, A. (2022). Judicial review and security governance: The Council of State and Greece's PNR implementation. European Constitutional Law Review, 18(2), 287–311.
Vidino, L., Marone, F., & Entenmann, E. (2017). Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West. Milan: ISPI.