

RADICALISATION, EXTREMIST PROPAGANDA AND TRAFFICKING IN HUMAN BEINGS

Collection of analytical articles



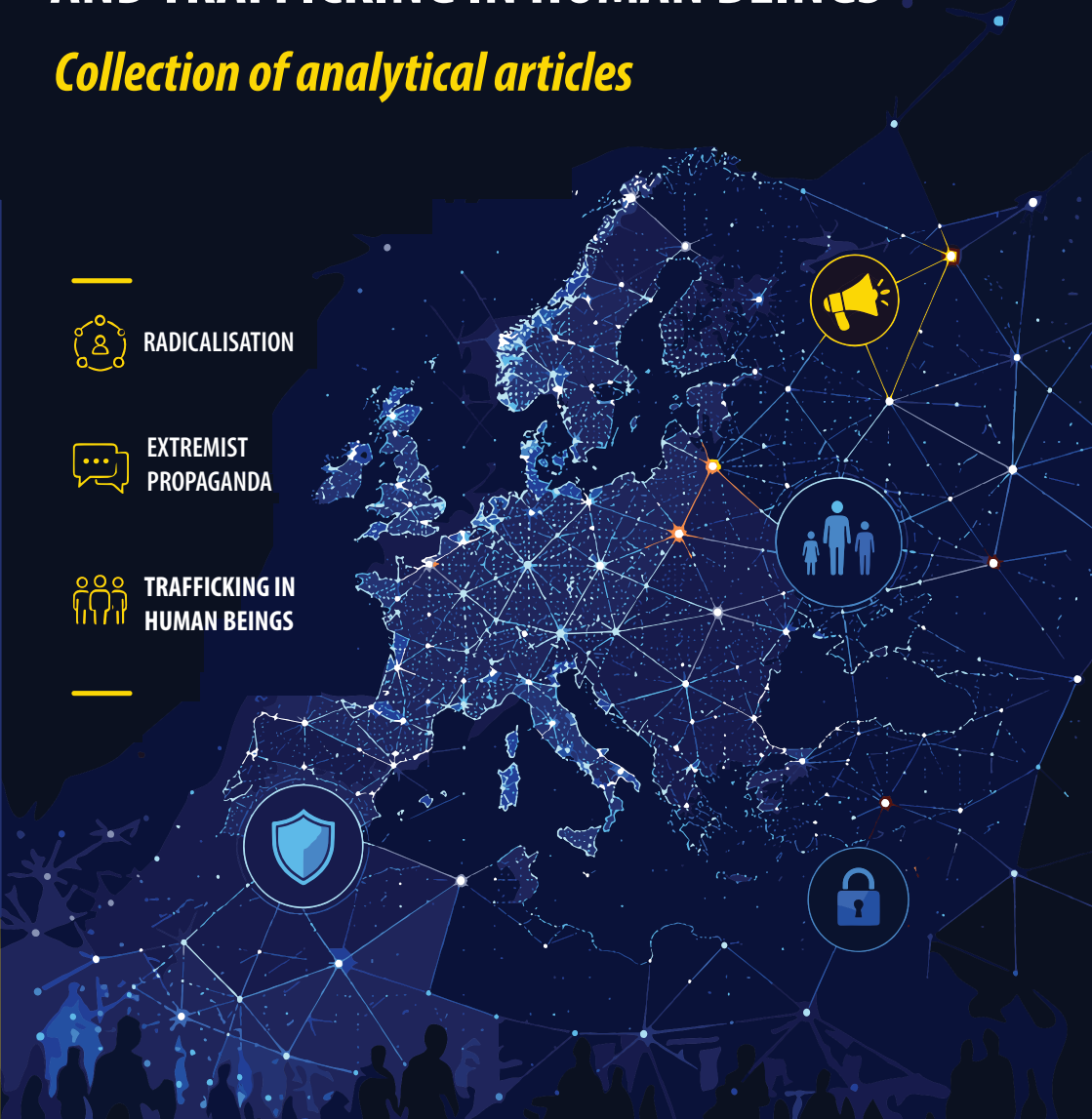
RADICALISATION



EXTREMIST
PROPAGANDA



TRAFFICKING IN
HUMAN BEINGS



Capacity building through exchange of good practices and research in
the security domain BG65ISPR001-3.004-0002



Co-funded by
the European Union

RADICALISATION, EXTREMIST PROPAGANDA AND TRAFFICKING OF HUMAN BEINGS

Collection of analytical articles



SOFIA, 2026



Co-funded by
the European Union

RADICALISATION, EXTREMIST PROPAGANDA AND TRAFFICKING OF HUMAN BEINGS

Collection of analytical articles

Authors: Barbara Lucini, Andrew Staniforth, Ruza Karlovic, Holger Nitsch, Holger Schmidt, Nadya Dimitrova, Antoaneta Vasileva, Borislav Mavrov, Iliyana Semerdzhieva.

Borislav Mavrov, editor

European Institute, layout

European Institute Foundation, Sofia 2026

ISBN

First edition

These analytical articles have been developed as part of the project “Capacity building through exchange of good practices and research in the security domain” No. BG65ISPR001-3.004-0002, Contract No. 812108-68-02.10.2024, funded by the Program of the Republic of Bulgaria under the Internal Security Fund 2021-2027.

The content of this material does not reflect the official opinion of the European Union and the Responsible Managing Authority. Responsibility for the information and views expressed in the document lies with its author and the European Institute Foundation.



CONTENTS

INTRODUCTION	5
NAVIGATING THE NOISE: REDEFINING SECURITY AMIDST VOLATILE RADICALISATION DYNAMICS	8
RADICALIZATION PREVENTION INITIATIVES IN SCHOOLS, COLLEGES AND UNIVERSITIES IN THE UK	39
PREVENTION BEFORE REPRESSION: HOW POLICE–COMMUNITY COLLABORATION ENHANCES PUBLIC SAFETY AND SECURITY	62
THE ROLE OF SOCIAL MEDIA FOR EXTREMIST ORGANISATIONS	77
HOW DO RELIGIOUSLY EXTREMIST ACTORS USE ONLINE ENVIRONMENTS FOR RECRUITMENT - AND WHAT CONCLUSIONS CAN BE DRAWN FROM THIS FOR POLICE PREVENTION WORK?	98
EUROPOL'S ENHANCED ROLE IN COMBATING MIGRANT SMUGGLING AND HUMAN TRAFFICKING	133
TECHNOLOGY-FACILITATED TRAFFICKING IN HUMAN BEINGS: EMERGING RISKS, INSTITUTIONAL RESPONSES AND POLICY CHALLENGES	153
HOW CLIMATE CHANGE SHAPES MIGRATION AND HUMAN TRAFFICKING. REFLECTIONS AND OBSERVATIONS	191



Co-funded by
the European Union



INTRODUCTION

Nowadays, more than ever, it is necessary to collect data and analyze it profoundly, to advance security-related research toward its full-scale implementation, and expand its scope to include new fields of research, which are oftentimes neglected. Only in this way can the actual work of law enforcement practitioners be supported, so that they are better prepared—not merely to respond to emerging threats, but to anticipate and manage them in a timely manner in line with the dynamics of the present-day environment.

This collection brings together eight analytical articles developed under the project “Capacity building through exchange of good practices and research in the security domain”. These publications are part of one of the key project activities aimed at establishing an international Center of Excellence in the security domain, conceived as a platform for integrating knowledge, exchanging best practices, and fostering dialogue among the academic community, practitioners, and institutions.

This collection presents the findings of the analytical work of established experts from Bulgaria and abroad, who examine three key thematic areas: radicalisation, extremist propaganda, and human trafficking. All publications share the goal to apply a critical interdisciplinary approach and the search for practical solutions and recommendations for policy changes in the context of a rapidly evolving security domain.

The first thematic area is devoted to radicalisation and its contemporary manifestations. The articles in this area examine radicalisation processes in the context of present-day social and institutional challenges, the role of the educational environment, early prevention, and the need for coordinated policies to mitigate risks among vulnerable groups. Em-



phasis is placed on preventive mechanisms, building resilience and the importance of partnerships between institutions, communities, and educational structures.

The second thematic area is focused on extremist propaganda and the use of the digital environment as a tool for influence, recruitment and dissemination of radical ideologies. The analyses in this section examine social media and online platforms as spaces where extremist messages are adapted and disseminated at high speed and with wide reach. Special attention is given to the challenges that institutions face in countering online radicalisation, as well as to the need for a balanced approach between ensuring security and protecting fundamental rights and freedoms.

The third thematic area covers topics such as smuggling and human trafficking, emphasizing the interconnection between these two phenomena and the need for change at institutional level. In-depth examination is also offered of the impact of digitalization, the cross-border nature of crime, and the need to adapt institutional and legal mechanisms to new forms of exploitation. The articles analyze how technologies change the patterns of committing and concealing crimes, expanding the circle of vulnerable individuals, and requiring new forms of international cooperation. This thematic strand also examines broader interconnections—between climate change, migration, and human trafficking—that open up new horizons for research.

The articles in these three thematic areas highlight the complex and interconnected nature of today's security challenges. Whether addressing radicalisation, extremist propaganda or human trafficking, all publications call for the need of an integrated, multidisciplinary and knowledge-based approach.

The collection's value is further enhanced by its team of authors—a unique combination of experts from academic circles, including police academies, practitioners from law enforcement agencies, researchers, analysts,



and representatives of the non-governmental sector. What they have in common is their extensive experience gained by their involvement in major international research projects in the security domain and their commitment to further advance the knowledge and policies in this domain.

This collection aims not only to present the project outcomes, but also to pave the way for future research, policies and practical initiatives. This approach lays the groundwork for a better-prepared, sustainable, and future-oriented Europe. We hope the collection will be useful both to specialists and to anyone seeking a deeper understanding of contemporary processes. In this sense, it is just the beginning—the first step in a broader series of analytical publications that the Center for Excellence in the security domain is set to develop.

Enjoy your reading!

The team of the European Institute Foundation



Co-funded by
the European Union

NAVIGATING THE NOISE: REDEFINING SECURITY AMIDST VOLATILE RADICALISATION DYNAMICS

Barbara Lucini



Abstract

Terrorist This paper aims to propose an analysis of the concept and phenomenon of radicalization by advancing a perspective grounded in the consideration of its evolution over the past twenty years, one that can incorporate the most significant changes and current trends from both a social and national and international security standpoint.

The purpose of this contribution is to provide a reflection on theoretical and methodological approaches to the phenomena of radicalization and violent extremism, with a particular focus on European policies and on the Italian case.

This is expected to be particularly useful for those directly involved in the management of such phenomena, as well as for those seeking to better understand the underlying dynamics that expose a large portion of contemporary societies to the risk of radicalization and to conditions of vulnerability.

Keywords: radicalisation; violent extremism; policy; PCVE; security.



1. Introduction – The catalyst for change

Contemporary societies have undergone profound changes with the advent of the COVID-19 pandemic, which has established new social dynamics and different modes of interaction in environments that are no longer exclusively offline but also online, highlighting a shift toward a multidimensional, digital way of life (Lucini, 2021).

This has also influenced certain polarizing and radicalizing trends that now appear to be consolidated in most European countries, as well as the increasingly prominent role that new technologies have assumed in fostering involvement in extremist attitudes and radical behaviors.

The phenomenon of radicalization thus becomes a central issue to address, especially about its definition and the various interpretations that, starting from how the phenomenon is defined, are used to guide policies of prevention, de-radicalization, and counteraction.

The changes that have occurred in European societies in the post-pandemic years must be considered as bringing about a new and necessary perspective for understanding these phenomena and the polarizing and violent tendencies that are becoming increasingly widespread.

In this deeply volatile new scenario, a new security framework represents a central element for the governance of countries and their stability.

The systematization of the evolution of these radical phenomena can also be observed through consideration of the results obtained from two different European research projects in which the author has worked.

The first concerns the EU Horizon 2020 project TRIVALENT – Terrorism pReventIon Via rAdicalisation countEr-NarraTive – in which considerable attention was devoted to the communicative dimension of Islamic religious and political extremism, subsequently focusing the operational proposal on two essential policy elements represented by alternative narratives and counter-narratives.



The second, the EU Horizon 2020 project COUNTER – Countering Radicalisation for a Safer World: Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection – focuses on the results of analyses and research carried out, which have shown, from an operational and methodological perspective, that current tools for preventing and understanding the threat of radicalization and violent extremism, namely TRA-Is (Terrorism Risk Assessment Tools), are no longer suitable for the social context in which they should be applied.

It is along this line, and with the aim of better understanding current and future policy orientations, that this contribution develops.

It begins with an in-depth examination of the different definitions of radicalization and the emergence of this concept, followed by an analysis and discussion of various policy approaches in European countries, with a focus on the Italian context.

Finally, future perspectives will be outlined both regarding the evolution of the threat and the prevention and management tools that appear most suitable and appropriate for the new international scenario and the current social context (Daher et al., 2025).



2. Radicalisation: defining the risk and navigating the noise

The concept of radicalisation is not new; it is rooted in the radical conception of 19th-century British political reform and subsequently emerged within the international landscape of the First World War. Throughout historical evolution, depending on the socio-political context, radicalisation and violent extremism have demonstrated their presence and destabilising impact on the governments and populations subjected to their effects.

In Europe and, more broadly, in Western countries, the concept of radicalisation systematically re-emerged following the attacks in the United States on September 11, 2001. From this point forward, both the public narrative promoted through various media channels and the political and legislative orientations adopted to manage the phenomenon began to disseminate the phrase “Islamic radicalisation,” associating it with specific ideological, religious, and cultural characteristics.

Consequently, for public opinion, the concept of radicalisation was transformed into an exclusive category pertaining to Islamic terrorism and religious extremism. Despite this sharp distinction in the definition of the concept, a wide range of diverse reflections emerged to address the question of what radicalisation entails, examined through psychological, sociological, political, and economic lenses. These factors are considered in relation to specific contexts and social environments where individuals may be exposed to the risk of radicalisation.

From a theoretical-academic perspective, Sedgwick (2010) argues that the term “radicalisation” depends on the formal context in which it is adopted—be it security, social integration, or foreign policy—thereby highlighting the multidimensional nature of the fields affected by the same radical phenomenon. This characteristic brings to light certain elements of conceptual confusion which are mirrored in the policy and legislative lines designed to manage and counter the phenomenon. In this regard, Neumann (2013) also emphasises the lack of a common definition and identifies a significant distinction: radicalisation can be recognised as cog-



nitive radicalisation, based on extremist beliefs and ideas, or identified as *behavioural radicalisation*, founded on extremist actions. The distinction maintained is therefore between extremist thought and the commission of, or participation in, extremist and terrorist acts.

In this field, a more operational perspective to overcome definitional confusion is proposed by McCauley & Moskaleiko (2008; 2011; 2017; 2020) with the *Two-Pyramids model*, which distinguishes between the radicalisation of opinions and ideas and the radicalisation of actions and behaviours. These two trajectories of radicalisation inform and constitute different methods of prevention, management, and response depending on the category to which an individual belongs. Furthermore, McCauley & Moskaleiko (2017), in their critical reflection on the definition of radicalisation, cite the work of Moghaddam (2005) who:

in “The Staircase to Terrorism,” offered an early metaphor of radicalization as a six-floor ever-narrowing stairway to terrorism. The ground floor is perception of injustice and relative deprivation; the first floor is search for options; the second floor is anger at the perceived perpetrators of injustice; the third floor is a moral engagement that justifies terrorism; the fourth floor is joining a terrorist group; and the fifth and last floor is dehumanizing enemy civilians to make them legitimate targets of violence. [...] The difference between justifying terrorism (third floor) and joining a terrorist group (fourth floor) is the difference between radical opinion and radical action. This key difference appears as just one more step in the staircase model.

This individual perspective, used to understand the concept of radicalisation and its underlying dynamics, constitutes the core of the theoretical and academic production in radicalisation studies. In subsequent years, it would direct the consideration of micro, meso, and macro approaches to the phenomena of radicalisation and extremism. Additionally, it should be noted that studies during those initial years of definitional reflection followed two theoretical lines.

The first is predominantly individualistic, from which profiling guidelines were structured from a methodological perspective, as the radicalised in-



dividual was at the centre of the phenomenon and had to be understood through their specific psychological and mental attitudes (Horgan 2005; 2014). From an operational perspective, this led to the development of TRA-Is (Terrorism Risk Assessment Tools) aimed at operationalising risk assessment and addressing the need to understand extremism and radicalisation risk for both prevention and de-radicalisation purposes (Lucini, 2023; 2024).

The second perspective is represented by the work of Wiktorowicz (2005), who focuses on radicalisation as an expression of social movements and social processes, highlighting the social nature of the radical phenomenon and the relevance of social identity construction in relation to the reference social network. The work of Della Porta and LaFree (2012) follows this perspective of considering radicalisation through the lens of social movements.

These two orientations have been, and remain, the primary pathways of theoretical debate regarding the definition of radicalisation and violent extremism, considering the influence of the disciplinary backgrounds of various scholars (e.g., psychology, sociology, criminology, political science). In later years, technological, political, social, and cultural changes—and more generally the international scenario—led to a broadening and further characterisation of these perspectives.

Specifically, there is a persistence of linear models and those predominantly oriented toward the individual path toward radical views and extremist behaviours. Alongside these, however, other studies have emerged regarding the definition of radicalisation and the understanding of dynamics and factors that can support such a phenomenon. In this regard, it is worth noting authors such as Cherif, R., et al. (2009), Borum (2011; 2014), Doosje et al. (2016), Hardy (2018), Van den Bos, K. (2018), and Schmid, A. P. (2013), who focus on possible pathways and models of radicalisation and extremism. Regarding specific risk factors and indicators, it is important to cite the studies by Lösel et al. (2018), Vergani et al. (2020), Kruglanski et al. (2019), Wolfowicz et al. (2020), and Duindam et



al. (2025), which focus on different factors that can attract, sustain, and promote radicalisation processes, as well as provide a better understanding of their role in both off-line and on-line recruitment dynamics.

The theoretical perspectives offered raise an essential question for the definitions of radicalisation and violent extremism regarding the role of violence, as highlighted by Bartlett et al. (2010), cited by McCauley and Moskalenko (2017): *“Becoming a terrorist was not always a natural or linear progression from being a radical. Those who turned to violence often followed a path of radicalisation which was characterised by a culture of violence, in-group peer pressure, and an internal code of honour where violence can be a route to accruing status. [...]”*

Bartlett and colleagues clearly emphasise that the path to becoming a terrorist does not follow a single trajectory with predefined factors. On the contrary, the construction of this identity lies in a complex, multidimensional journey in which various factors combine differently depending on the context and the technological access possessed by the individual or groups.

A more general point relative to the theoretical lines previously highlighted is represented by the definition of the phenomenon of radicalisation found in the *Commission Implementing Regulation (EU) 2019/103* (European Commission, 2019), which defines radicalisation as follows:

“‘radicalisation’ means the phenomenon of socialisation to extremism of people embracing opinions, views and ideas, which could lead to terrorism.”

This definition is useful for defining a crucial characteristic of radicalisation: that it is a dynamic, vital, and continuously transforming process that permeates the mechanisms and dynamics of socialisation. These may fall within the sphere of primary socialisation (occurring in the family context) or within broader socialisation that includes different actors such as schools, peer groups, other reference adults, and—for nearly two decades now—new technologies and the world of social media communication. Indeed, it is this new actor that provides a novel perspective for understanding the phenomena of radicalisation and violent extremism.



3. Radicalisation: current and future perspectives

The increasingly growing social complexity, the interdependence of technological infrastructures that have become indispensable, and international scenarios of increasing vulnerability and uncertainty have led to a profound transformation in the processes of radicalisation and in the dynamics that may lead individuals or social groups towards violent extremism and, consequently, to the perpetration of terrorist attacks that are highly destabilising for personal, national, and international security.

In this highly intricate framework, it should not be overlooked that the advent of the pandemic in 2020 redefined the global social milieu, leading to a significant reconfiguration of social relations, both among individuals and between individuals and institutions, which also includes processes of radicalisation and phenomena of violent extremism.

In particular, references to the previous literature developed on these topics have shown how the evolution in the understanding and definition of these phenomena varies in accordance with governance, legislative, and technological elements. The technological evolution of communication media has, over the last two decades, enabled important changes concerning the role of the public within media consumption contexts, shifting from a passive audience to an active one and a co-producer of digital content.

In this context, it has become evident to conceive processes of radicalisation as communicative and relational phenomena, focusing attention on the digital contexts in which these phenomena are activated and develop, considering the new dimension of life that, for most individuals, is situated in a hybrid zone between the off-line and the online dimension (Vergine et al., 2024). In particular, the online dimension has been the subject of various studies (Conway, 2017; 2021; Ledwich and Zaitsev, 2019; Lavie-Driver and van der Linden, 2025; Núñez-Guerra, 2025) that have examined in depth the role of new technologies considered as both means and environments in which extremist individuals or those with



initial polarising beliefs may find and disseminate radical and extremist materials and information aimed at recruitment and at the structuring of networks around the same or similar extremist ideologies.

In this context of study and research, a reflection has developed based on the results of several research projects for which Lombardi, Maiolino and Lucini (2020) and Lombardi and Lucini (2021) conceptualised a new perspective with the aim of better understanding and delineating the phenomenon of online radicalisation, developing the perspective of the FORMAT model. Through this perspective, a certain type of static conception of the network is overcome—according to which what occurs online remains confined to that dimension—and a communicative alternative is proposed to the approach of alternative narratives and counter-narratives that had, for several years, dominated prevention and counteraction activities related to processes of radicalisation and violent extremism.

The FORMAT model proposes a different paradigm centred on the communicative dimension of phenomena of polarisation and extremism, focusing on: “The format model is constituted by two key elements such as communication ecosystem and narrative-scape.” (Lombardi, Maiolino and Lucini, 2020), thereby highlighting, for the first time, the central role played by communication ecosystems and narrative-scapes: from being merely media and technological contexts, they become key actors in processes of polarisation, radicalisation, and extremism.

In accordance with this reflection, the transition also occurs across different levels of analysis, insofar as the first—developed by various institutional and social actors—focused on prevention with particular attention to individual narratives circulating online and therefore on the construction of alternative or counter-narratives; the FORMAT model, instead, shifts the level of analysis to the media context, understood no longer as a passive actor but as a crucial element for the prevention and countering of radicalisation. In particular, “The format is a media-cultural product consisting of communication guidelines to implement when considering feelings, emotions, perceptions of an audience; types of narrations; fea-



tures of the current scenario and narrative-scapes adapted to the single communication ecosystem and for the specific purpose of the communication process.” (Lombardi, Maiolino and Lucini, 2020).

This perspective highlights and anticipates by several years the specific attention that will be paid to new processes of radicalisation, risk scenarios, and novel elements (Lucini, 2024^o; 2025a; 2025b), such as:

- radicalisation processes are situated within a digital dimension that encompasses both the off-line and the on-line dimensions, resulting in the new term proposed by Floridi (2014), namely on-life. Radicalisation thus assumes both a cognitive and an emotional connotation, which become central within the new context of digital communication ecosystems. In particular, the cognitive dimension is especially relevant for the interaction that potentially vulnerable individuals and groups have with the digital environment and with platform tools and artificial intelligence. In accordance with this perspective, propaganda and recruitment activities (Lucini, 2022) are facilitated. The latter have also been studied from the perspective of vetting, and therefore of a selection–filtering process
- the context in which dynamics of radicalisation and violent extremism develop, including through phenomena such as hate speech or the polarisation of discourse, becomes a central actor that can be recognised in the characteristics of pervasiveness, permanence, and interdependence typical of digital communication ecosystems (Lucini, 2024b). This is also evident from the shift in focus from specific radicalisation factors rooted in the sphere of mental health and structural vulnerabilities (familial, socio-educational, economic-labour) towards consideration of the role that communicative dynamics and relationships play in sustaining polarised and radical attitudes, ideas, and behaviours;
- another central element in this new perspective on the phenomenon of radicalisation concerns ideological hybridisation or the volatile



ideological-cultural context in which polarising dynamics develop within digital communication ecosystems (Lucini, 2017): there are no longer models of purely ideological radicalisation, but rather an evident ideological blending that has been defined by various scholars as “salad-bar extremism” or also as phenomena of double radicalisation, whereby some individuals radicalise according to one ideology and subsequently change orientation to embrace extremist cultural approaches of an opposite nature. Examples in this regard include cases of ideological fusion such as the phenomenon of narrative syncretism between accelerationists and salafi-jihadists as studied by Argentino et al. (2022), and that of “Composite Violent Extremism” coined by Gartenstein-Ross et al. (2022);

- a necessary revision of terrorism assessment tools – TRA-Is in order to align them with new forms of radicalisation and extremism, thus making them current and resilient with respect to ongoing social changes (Lucini, 2023; 2024c; Lahnala et al., 2025);
- youth and minors emerge as a specific target for dynamics of radicalisation and extremism, with certain trends that are progressively consolidating;
- the impact that the geopolitical and international situation has on the stability and security of various countries, their governments, and populations, as well as on polarising digital dynamics, extremist communication, and social radicalisation

These new elements emerging from the analysis of the definition and the different conceptualisations of the phenomenon and processes of radicalisation confirm the context-sensitive nature of the phenomenon and the need to examine in detail policy analyses for the prevention and countering of radicalisation and extremism promoted by various institutional agencies of the European Union, with the aim of better understanding the influence that underlying theoretical paradigms have in shaping the understanding of social phenomena and the future perspectives that may emerge.



4. Policies for prevention and countering radicalisation and extremism

Prevention, management, and countering strategies and policies addressing phenomena of radicalisation, violent extremism, and terrorism have been systematised since the early 2000s following the spread of attacks carried out in the United States and Europe by Islamist extremists.

Strategic orientations and operational practices are influenced by the typology of the phenomena and by the characteristics of contemporary threat.

In considering the architecture of legislative perspectives and policies, it is necessary to recall the theoretical framework and its evolution as previously discussed, which highlights key features of the phenomenon that guide operational applications and the activities implemented for the purposes of prevention, management, and countering of radicalisation processes and violent extremism.

In this regard, it is possible to identify several fundamental phases of these orientations and the practices they have generated.

Indeed, in the early 2000s up to approximately 2010, strategic orientations focused on intelligence activities and on a predominantly defensive security approach. These were years characterised by efforts to understand the threat from an international perspective and with the aim of better comprehending its dynamics. In the subsequent five years, an orientation towards networking capacity and information-sharing among agencies and law enforcement at the European level prevailed, highlighting the need to share common technological systems for information exchange, as well as linguistic and cultural codes that would enable dialogue among Member States and their security agencies. Subsequently, and up to the 2020s, there has been a predominance of operational approaches linked to technological evolution and to the exploitation by extremist actors of the



online dimension and the opportunities it offers for recruitment, dissemination, and sharing of extremist materials and information. These are also the years in which, from a theoretical perspective, the role of ideologies begins to weaken in radical and extremist scenarios, giving way to more diverse forms of extremism with varying ideological bases and with phenomena of double or multiple radicalisation.

During this period, policy orientations are therefore directed towards a greater understanding of the threat and of its exploitation of the internet for purposes of destabilisation, propaganda, and dissemination of extremist material. Moreover, considering the emerging ideological–cultural diversity, multi-agency approaches are supported for prevention activities, to manage the complexity of the threat and the multiple risk factors that are increasingly consolidating, including within the online dimension.

Finally, in the most recent years, starting from 2020, the previous perspective has been consolidated, with an even stronger focus on digital security and on the governance of extremist phenomena that now develop through a continuous interweaving of the offline and online dimensions.

The threat thus becomes hybrid both in its ideological–cultural characteristics and in its use of digital technologies for extremist purposes and for domestic and international terrorism.

The figure below summarises the essential milestones in the evolution of European policies on radicalisation and violent extremism.

More specifically, the first communications of the European Commission framed the phenomenon within the domain of security and prevention, culminating in the Strategy for Combating Radicalisation and Recruitment in its revised and final form in 2014, which also included the phenomenon of foreign fighters, considered at that time as a key element in radicalisation dynamics and in the events that occurred. The development of the Radicalisation Awareness Network (RAN) in 2011—which in 2024 became the EU Knowledge Hub—demonstrates the relevance of a net-



Figure 1 – Timeline EU policies on radicalisation and violent extremism. Source: Generated with ChatGPT (OpenAI), 2026

work-based and multi-agency approach for the study and understanding of increasingly complex and rapidly evolving threats and risks, particularly in light of technological evolution and the opportunities it offers in terms of recruitment, organisation, and dissemination of extremist and radical ideas.



The year 2020 marks the point at which the European Union systematised its approach through the Security Union Strategy (European Commission, 2020a) and the Counter-Terrorism Agenda (European Commission, 2020b), which consider activities of anticipation, prevention, protection, and response, identifying radicalisation as a complex, multidimensional phenomenon rooted in a social dimension, the understanding of which requires further in-depth analysis.

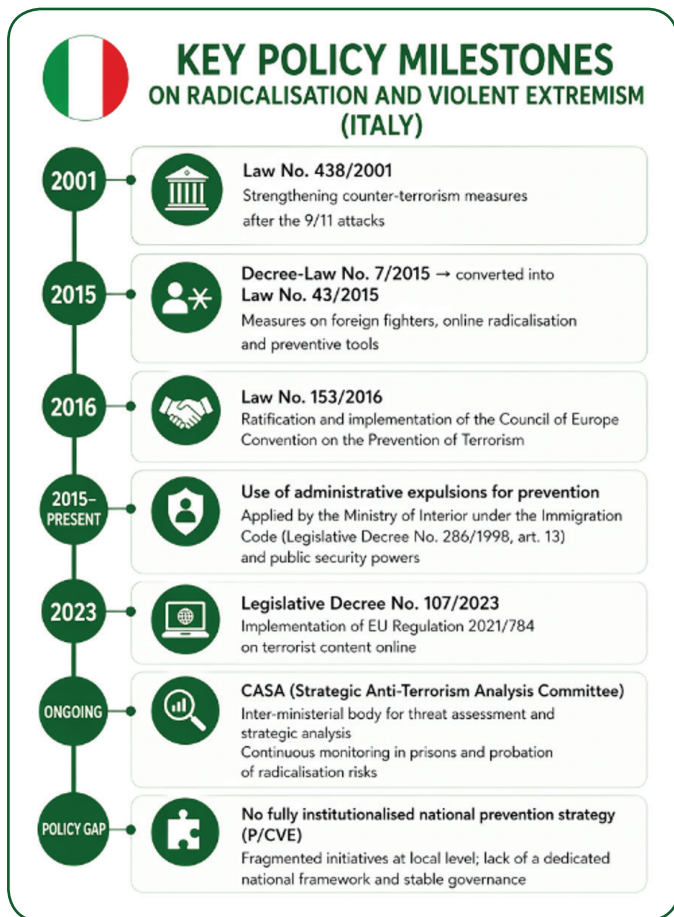
Technological evolution and the digital dimension are addressed in relation to the ways in which extremist individuals and groups may exploit them, notably with the adoption of Regulation (EU) 2021/784, which focuses on the security of the digital environment and the protection of fundamental rights.

In recent years, the European policy framework for the prevention, management, and countering of radicalisation and violent extremism appears to be oriented towards a greater awareness of the complexity of the threat and its destabilising characteristics, emphasising the need for a multi-level approach and for coordinated prevention policies capable of supporting the management of risk and extremist threats.

This framework is not without limitations and vulnerabilities, for instance regarding the need to harmonise legal and operational frameworks across different European countries.

In this regard, and by way of example, the Italian case may be considered, which appears particularly distinctive given the country's specific national history in the prevention of and fight against organised crime.

The figure below illustrates the temporal evolution of the policies adopted by Italy for the management of phenomena of radicalisation and violent extremism.



*Figure 2 – Timeline Italian policies on radicalisation and violent extremism.
Source: Generated with ChatGPT (OpenAI), 2026*

The Italian model develops along key milestones that illustrate the progressive adoption of European legislative and policy frameworks, resulting in a robust legal apparatus but a weaker implementation of prevention strategies.



From 2015 onwards and in subsequent years, priorities for Italy also include the consideration of the phenomenon of foreign fighters and online radicalisation as a new environment for the dissemination and development of increasingly ideologically diverse forms of extremism.

Furthermore, with regard to the Italian case, it is important to highlight the establishment of the Strategic Anti-Terrorism Analysis Committee (CASA) in 2004, which formalised a policy orientation centred on the need for networking among different security agencies and on the primary focus of information-sharing. This also underscores the necessity of a communicative context that not only shares common perspectives but also linguistic and cultural codes that enable the multiple professional actors involved to understand each other effectively and to translate their activities into effective preventive and countering policy practices.

The Italian case is also useful in emphasising the need to better structure and systematise national prevention and countering strategies (P/CVE), in light of the local fragmentation and dispersion that are often associated with such initiatives and activities, not only in Italy.

Finally, the ultimate objective of policy frameworks, both at the European level and within individual Member States, should be to translate into policy orientations the significant social transformations taking place in European societies, which increasingly involve forms of radicalisation that are diffuse and volatile, and therefore difficult to define in terms of specific ideological characteristics and cultural reference systems.



5. Recommendations and Conclusion

The presentation of the crucial aspects emerging from the different theoretical approaches to the definition of radicalisation and violent extremism, as well as the evolutionary overview of European policies for the prevention and countering of forms of radicalisation and extremism, makes it possible to reach several essential considerations that are useful for better capturing the “noise” referred to in the title, which can be understood as a contemporary multiplicity of forms of radicalisation characterised by a low degree of ideological orientation, multidimensionality, and volatility in their evolution.

The first aspect to be emphasised, therefore, is the need to redefine security approaches and the related policies in order to better propose guidelines and prevention and countering activities that are aligned with the historical, political, cultural, economic, and social transformations of contemporary societies and that take into account the characteristics of the current threat. This is related to the awareness that the concept of radicalisation, from both a theoretical and an identificatory perspective, cannot be defined a priori nor taken as given, as demonstrated by contemporary events; rather, it confirms its context-sensitive nature. This characteristic is precisely the reason why, as previously discussed, it becomes necessary to focus on the context and on the central role it plays in processes of radicalisation and in the dynamics of violent extremism.

In this regard, the context is also shaped by the representation provided by institutional agencies and digital media, taking into account the effects that such representations have on the perception of these phenomena and of their transformations.

By way of example, one may consider the two reports produced in 2025 by Europol (EU TE-SAT) and the European Institute for Counter Terrorism and Conflict Prevention (EICTP), which combine an analysis of radicalisation, terrorism, and violent extremism trends using both empirical data and predictive analysis.



An important finding emerging from both reports is the decrease in terrorist attacks in Europe; however, alongside this trend, there is also the previously identified tendency of an emerging threat that is increasingly complex, interconnected with multiple variables, and more difficult to predict.

Both reports highlight growing concern regarding the use of digital technologies and the ways in which extremist groups and radicalised individuals may exploit them to disseminate content and recruit potential future radicals, thereby transcending ideological boundaries and rendering this threat similar across different ideological perspectives.

Significant differences between the two reports also emerge, which are useful for understanding the security approaches necessary to reconfigure strategic and policy frameworks in light of evolving threats.

Specifically, the two reports differ in their methodological approaches: the Europol report is based on a data-driven analysis, whereas the EICTP report proposes a predictive analysis oriented towards future developments. Moreover, the latter considers threats arising from the complex and challenging international context, viewing geopolitical scenarios as potential risk factors and sources of instability for European societies.

What emerges very clearly is a transformation in the nature of the threat, which appears significantly less defined by a specific ideological perspective, increasingly technology-oriented, and capable of absorbing the destabilising potential stemming from international tensions and conflicts, thereby intercepting vulnerabilities that are partly latent within European countries.

Starting from the consideration that the context of digital communication ecosystems (Lucini, 2024) represents the scenario understood as a proactive actor in current radicalisation processes, it becomes necessary to better understand which policy orientations should be adopted, considering their evolution and potential.

Over the years of their implementation, policies for the prevention and countering of radicalisation and extremism have revealed several methodological and operational limitations:



- a weakness in design (Charkawi et al., 2024), which is reflected in methodological implementation, due to the lack of standardised indicators that can be replicated across different contexts for which they were developed, as well as difficulties in measurement;
- difficulties in evaluating effectiveness, both for prevention programmes and for countering initiatives, due to methodological challenges in measuring their actual impact (Milbradt and Greuel, 2024; Ludden et al., 2022; Hofman et al., 2018);
- fragmentation in the design and implementation of policies and programmes across different European countries (Antonelli et al., 2024)

These aspects need to be more thoroughly considered within the European security approach, given their implications for understanding the effectiveness of prevention and countering programmes related to radicalisation.

More specifically, several elements emerge as priorities, concerning both the theoretical and the methodological–operational dimensions.

With regard to the theoretical perspective, there is a need to deepen knowledge of current radicalisation processes and the socio-cultural dynamics underlying them.

The ideological indifferentiation of current forms of radicalisation signals a significant transformation of the threat that requires further definition, also in order to provide law enforcement agencies and stakeholders with linguistic and cultural codes through which cooperation among different actors can be effectively implemented, in line with the multi-agency logic that remains a core European policy orientation.

In this context, it is also necessary to reconsider the role of emotional drivers (Lucini, 2025a) in contemporary radicalisation and how these activate radicalisation processes and extremist phenomena among minors, who can be considered the primary target of prevention interventions and programmes, particularly with regard to the use of social media and new artificial intelligence technologies.



Contemporary radicalisation is in fact diffuse and activated by perceptions, emotions, and personal interpretations that are not always linked to, or attributable to, specific ideological value systems and extremist groups. From this perspective, the threat appears more subtle and more difficult to predict; however, this should not lead to abandoning the possibility of continuous monitoring and the identification of behavioural patterns which, if adequately contextualised, may provide a certain level of predictability.

With regard to the methodological and operational perspective, a revision of the security paradigm adopted thus far is required, as the emerging threat is configured as multi-layered. As such, a new paradigm for prevention and countering should be identified that takes this characteristic into account as a necessary evolution of the previous multi-agency approach. The latter remains fundamental within this new framework, as the nature of the threat involves a variety of actors, and therefore inter-agency collaboration constitutes a cornerstone of prevention and countering strategies.

At the operational level, a revision of current prevention and countering programmes for radicalisation is required, taking into account changes in the nature of threats, the limitations in effectiveness and evaluation of programmes implemented thus far, and the introduction of horizon scanning activities typical of risk management approaches. Such activities could prove highly useful for understanding radicalisation and extremism dynamics in contexts characterised by low specific ideological orientation but high multidimensional vulnerability.

Finally, with regard to specific policy orientations that may be subject to further analysis and discussion, the following can be identified:

- recognising the context, both national and international, not merely as a background or setting for social processes of radicalisation, but as an active actor capable of shaping the adoption of certain radical views and behaviours;



- recognising the volatile nature - and therefore the adaptive and resilient character - of radicalisation processes (Lucini, 2025b), understood as forms of extremist and radical socialisation that may result in violent behaviour and terrorist acts;
- recognising the communicative dimension (Lucini, 2024) as central both to the identification and monitoring of the threat and to its subsequent management and countering;
- acknowledging that the specific communicative dimension, which also pertains to law enforcement agencies, is linked to the need to consider the impact and opportunities created by new technological tools;
- overcoming the limitations identified in the implementation of prevention and countering programmes by placing greater emphasis on the possible standardisation of policy design and their interventions;
- training as a fundamental element, along with the promotion of programmes - for example for law enforcement agencies, civil society, and stakeholders - focused on the evolving nature of the threat, the role of new technologies, and potential methodologies for prevention and countering programmes.

This represents an opportunity to integrate multi-agency and multi-layer security perspectives, leading to a new understanding of current threats and of the methodologies for identifying, monitoring, preventing, and countering radicalisation processes and violent extremism.

Finally, in light of recent cases occurring in various European countries and the trends that appear to be increasingly confirmed, it is necessary to consider the youth population as a primary target for future initiatives related to training on the use of new technologies, in order to promote greater and broader awareness of the central and strategic role that communication plays in identity construction, in the dissemination of extremist and radical ideas, in recruitment, and in the organisation of acts of violent extremism and terrorism.



6. Bibliography

- Antonelli, F., Musolino, S., & Rosato, V. (2024). Preventing and countering violent extremism: A comparison between European countries. *International Review of Sociology*. <https://doi.org/10.1080/03906701.2024.2322329>
- Bartlett, J., Birdwell, J., & King, M. (2010). *The edge of violence: A radical approach to extremism*. London, United Kingdom: Demos.
- Borum, R. (2011). Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security*, 4(4), 7–36.
- Borum, R. (2011). Radicalization into violent extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security*, 4(4), 37–62.
- Borum, R. (2014). Psychological vulnerabilities and propensities for involvement in violent extremism. *Behavioral Sciences & the Law*, 32(3), 286–305.
- Bressan, S., Stoffel, S. L., & Heidrich, Z. Á. (2025). Trends in violent extremism, prevention and evaluation: Three years of international evidence (2023–2025). Global Public Policy Institute (GPPi). <https://gppi.net/2025/12/18/international-trends-in-violent-extremism-prevention-and-evaluation-2023-2025>
- Charkawi, W., Dunn, K., & Bliuc, A. M. (2024). Evaluations of countering violent extremism programs: Linking success to content, approach, setting, and participants. *International Journal of Law, Crime and Justice*, 77, 100674. <https://doi.org/10.1016/j.ijlcj.2024.100674>
- Cherif, R., Barley, K., & others. (2009). *Terrorism: Mechanisms of radicalization processes, control of contagion and counter-terrorist measures*. arXiv
- Conway, M. (2017). Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98. <https://doi.org/10.1080/1057610X.2016.1157408>
- Conway, M. (2021). Online extremism and terrorism. *Annual Review of*



Criminology, 4, 1–21.

- Daher, J., Antonelli, F., & Rosato, V. (2025). Social roots of violent extremism. Springer.

- Doosje, B., Moghaddam, F. M., Kruglanski, A. W., De Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. *Current Opinion in Psychology*, 11, 79–84.

- Duindam, H., et al. (2025). Protective factors against violent radicalization: A systematic review. *Aggression and Violent Behavior*.

- European Commission. (2019). Commission Implementing Regulation (EU) 2019/103 of 23 January 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security. *Official Journal of the European Union*, L 21, 24 January 2019.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:32019R0103>

- European Institute for Counter Terrorism and Conflict Prevention (EICTP). (2025). *European Trend Report on Terrorism 2025*. Vienna: EICTP.

Available at: <https://eictp.eu/en/european-trend-report-on-terrorism-2025/>

- Europol. (2025). *European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT)*. Luxembourg: Publications Office of the European Union.

- Available at: <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat>

- Floridi, L. (Ed.). (2014). *The onlife manifesto: Being human in a hyper-connected era*. Springer

- Gartenstein-Ross, D., et.al. (2024) *Composite Violent Extremism: A Radicalization Pattern Changing the Face of Terrorism in Lawfare*, 22 November 2022 <https://www.lawfaremedia.org/article/composite-violent-extremism-radicalization-pattern-changing-faceterrorism>

- Hardy, K. (2018). Comparing theories of radicalisation with countering



violent extremism policy. *Journal for Deradicalization*, (15), 76–110.

- Hofman, J., & Sutherland, A. (Eds.). (2018). *Evaluating interventions that prevent or counter violent extremism: A practical guide* (RR-2094). RAND Corporation. https://www.rand.org/pubs/research_reports/RR2094.htm

- Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American Psychologist*, 60(2), 161–169.

- Kruglanski, A. W., Bélanger, J. J., & Gunaratna, R. (2019). *The three pillars of radicalization: Needs, narratives, and networks*. Oxford University Press.

- Lahnlala, A., Varadarajan, V., Flek, L., Schwartz, H. A., & Boyd, R. L. (2025). Unifying the extremes: Developing a unified model for detecting and predicting extremist traits and radicalization. *Proceedings of the International AAAI Conference on Web and Social Media*, 19(1), 1051–1067. <https://doi.org/10.1609/icwsm.v19i1.35860>

- Lombardi, M., Maiolino, M., & Lucini, B. (2020). Beyond counter and alternative narratives to tackle extremism: The new Format model. *Sicurezza, Terrorismo e Società*, (11), 7–44.

- Lombardi, M., & Lucini, B. (2021). The Format and FEAR model as an answer to new radicalization challenges. In R. Corrado, G. Wössner, & A. Merari (Eds.), *Terrorism risk assessment instruments*. IOS Press.

- Lucini, B. (2017). Critica della radicalizzazione pura. *Forme ibride di radicalizzazione estremista. Sicurezza, Terrorismo e Società*, (6), 43–62.

- Lucini, B. (2021). Nuove forme di radicalizzazione religiosa e politica ai tempi della pandemia. *Rivista Trimestrale di Scienza dell'Amministrazione*, 4, 1–20.

- Lucini, B. (2022). Vetting e processi di radicalizzazione come pratiche di comunità digitali: dai TRA-I al metaverso. <https://publicatt.unicatt.it/handle/10807/232303>

- Lucini, B. (2023). Nuovi attacchi estremisti in Europa e strumenti di valutazione della minaccia: una riflessione critica sui TRA-Is. *ITSTIME*, Retrieved online: www.itstime.it

- Lucini, B. (Ed.). (2024a). *Radicalizzazione, estremismi e nuove minacce*. BTT Editori.



- Lucini, B. (2024b). La radicalizzazione e gli ecosistemi digitali comunicativi: una prospettiva sociologica. In B. Lucini (Ed.), *Radicalizzazione, estremismi e nuove minacce*. BTT Editori.
- Lucini, B. (2024c). I TRAI-s e gli strumenti di valutazione del rischio estremismo. In *Radicalizzazione, estremismi e nuove minacce* (pp. 139–167). New Press Edizioni.
- Lucini, B. (2025a). Emozioni e identità: Nuove prospettive per comprendere gli attuali fenomeni estremisti violenti e il terrorismo. ITSTIME.
<https://www.itstime.it/w/emozioni-e-identita-nuove-prospettive-per-comprendere-gli-attuali-fenomeni-extremisti-violenti-e-il-terrorismo-by-barbara-lucini/>
- Lucini, B. (2025b). Revised radicalisation: Nuovi scenari e prospettive future. ITSTIME.
<https://www.itstime.it/w/revised-radicalisation-nuovi-scenari-e-prospettive-future-by-barbara-lucini/>
- Ludden, V., Sharp, F., Cioanca, A., Aparicio Jodar, L., Vahovska, M., Laine, A.-M., Rasmussen, C. L., Bech, E. C., Rusmann, K., Uilcna, D., Carta, E., Davidovi, G., Zeisl, Y., Jover Plasencia, M., Shelton, P., & Giacomelli, G. (2022). Evaluation of impact and effectiveness of counter- and alternative campaigns stemming from the Civil Society Empowerment Programme (CSEP) aiming at preventing radicalisation leading to violent extremism and terrorism: Final report. European Commission, Directorate-General for Migration and Home Affairs. https://home-affairs.ec.europa.eu/system/files/2023-01/CSEP%20final%20report_en.pdf
- McCauley, C., & Moskalenko, S. (2008). Mechanisms of political radicalization. *Terrorism and Political Violence*, 20(3), 415–433.
- McCauley, C., & Moskalenko, S. (2011). *Friction: How radicalization happens to them and us*. Oxford University Press.
- McCauley, C., & Moskalenko, S. (2017). Understanding political radicalization: The two-pyramids model. *American Psychologist*, 72(3), 205–216. <https://doi.org/10.1037/amp0000062>
- McCauley, C. (2020). The ABC model of radicalization: A commentary from the perspective of the two-pyramids model. *Behavioral Sciences of*



Terrorism and Political Aggression, 12(1), 1–14. <https://doi.org/10.1080/19434472.2018.1460732>

- Milbradt, B., & Greuel, F. (2024). Mixed methods evaluation on programs of preventing and countering violent extremism: Basics, state of play, challenges (PrEval Expertise 5/2024). Peace Research Institute Frankfurt (PRIF). <https://doi.org/10.48809/PrEvalExp2405>

- Horgan, J. (2005). The psychology of terrorism. London, United Kingdom: Routledge.

- Horgan, J. (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. The ANNALS of the American Academy of Political and Social Science, 618(1), 80–94. <https://doi.org/10.1177/0002716208317539>

- Horgan, J. (2014). The psychology of terrorism (2nd ed.). Routledge.

- Lavie-Driver, N., & van der Linden, S. (2025). Social media, AI, and the rise of extremism during intergroup conflict. Frontiers in Social Psychology, 3, 1711791. <https://doi.org/10.3389/frsps.2025.1711791>

- Ledwich, M., & Zaitsev, A. (2019). Algorithmic extremism: Examining YouTube's rabbit hole of radicalization. arXiv. <https://arxiv.org/abs/1912.11211>

- Lösel, F., et al. (2018). Risk and protective factors in radicalization. International Journal of Conflict and Violence, 12.

- Wiktorowicz, Q. (2005). Radical Islam rising: Muslim extremism in the West. Oxford, United Kingdom: Rowman & Littlefield.

- Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2020). A field-wide systematic review and meta-analysis of putative risk and protective factors for radicalization outcomes.

Journal of Quantitative Criminology, 36(3), 407–447.

<https://doi.org/10.1007/s10940-019-09439-4> Lahnal, M., et al. (2025). Computational modeling of radicalization processes. Journal of Computational Social Science.

- Núñez-Guerra, C. (2025). The factor of social media and artificial intelligence in the radicalization of youth. In Lecture Notes in Computer Science (Vol. 15939). Springer. https://doi.org/10.1007/978-3-032-01429-0_9



- Kruglanski, A. W., Bélanger, J. J., & Gunaratna, R. (2019). *The three pillars of radicalization: Needs, narratives, and networks*. Oxford University Press.
- Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American Psychologist*, 60, 161–169. <http://dx.doi.org/10.1037/0003-066X.60.2.161>
- Neumann, P. (2013). The trouble with radicalization. *International Affairs*, 89(4), 873–893.
- Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. ICCT Research Paper.
- Sedgwick, M. (2010). The concept of radicalization as a source of confusion. *Terrorism and Political Violence*, 22(4), 479–494. <https://doi.org/10.1080/09546553.2010.491009>
- Van den Bos, K. (2018). *Why people radicalize: How unfairness judgments are used to fuel radical beliefs, extremist behaviors, and terrorism*. Oxford University Press.
- Vergani, M., Iqbal, M., Ilbahar, E., & Barton, G. (2020). The three Ps of radicalization: Push, pull and personal. *Studies in Conflict & Terrorism*, 43(10), 854–885.
- Vergine, I., Galimberti, C., Lucini, B., & Lombardi, M. (2024). Onlife subjectivities construction in two radicalized ecosystems: A practical application of a theoretical perspective. *Annual Review of Cybertherapy and Telemedicine*, 22, 55–59.



Appendix A - Sources of Timeline of EU policies on radicalisation and violent extremism. Source: Generated with ChatGPT (OpenAI), 2026

- European Commission. (2005). Terrorist recruitment: Addressing the factors contributing to violent radicalisation (COM(2005) 313 final).
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-52005DC0313>
- European Commission. (2011). Radicalisation Awareness Network (RAN).
https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran_en
- Council of the European Union. (2014). Revised EU strategy for combating radicalisation and recruitment to terrorism.
<https://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf>
- European Parliament and Council of the European Union. (2017). Directive (EU) 2017/541 on combating terrorism.
<https://eur-lex.europa.eu/eli/dir/2017/541/oj>
- European Commission. (2020a). EU Security Union Strategy (COM(2020) 605 final).
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-52020DC0605>
- European Commission. (2020b). A counter-terrorism agenda for the EU (COM(2020) 795 final).
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-52020DC0795>
- European Parliament and Council of the European Union. (2021). Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. <https://eur-lex.europa.eu/eli/reg/2021/784/oj>
- European Commission. (2024). EU Knowledge Hub on prevention of radicalisation.
https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/eu-knowledge-hub-prevention-radicalisation_en



- European Commission. (2025). ProtectEU: European internal security strategy (COM(2025) 148 final).

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-52025DC0148>

- European Commission. (2026). Internal Security Fund (ISF) 2026–2027 calls for proposals.

https://home-affairs.ec.europa.eu/funding/internal-security-fund_en

Appendix B - Sources of Timeline of EU policies on radicalisation and violent extremism. Source: Generated with ChatGPT (OpenAI), 2026

- Italian Republic. (1998). Decreto legislativo 25 luglio 1998, n. 286 (Testo unico immigrazione), art. 13. <https://www.normattiva.it>

- Italian Republic. (2001). Legge 15 dicembre 2001, n. 438.

<https://www.normattiva.it>

- Italian Republic. (2015). Decreto-legge 18 febbraio 2015, n. 7, convertito con modificazioni dalla Legge 17 aprile 2015, n. 43. <https://www.normattiva.it>

- Italian Republic. (2016). Legge 28 luglio 2016, n. 153. <https://www.normattiva.it>

- Italian Republic. (2023). Decreto legislativo 7 luglio 2023, n. 107.

<https://www.normattiva.it>

- Italian Government. (n.d.). Comitato di Analisi Strategica Antiterrorismo (CASA). <https://www.interno.gov.it>



RADICALIZATION PREVENTION INITIATIVES IN SCHOOLS, COLLEGES AND UNIVERSITIES IN THE UK

Andrew Staniforth



Abstract

Terrorist organizations operating across Europe today are intentionally targeting young people, and individuals as young as 13 have already been implicated in terrorist-related activity. Environments where young people frequent during their education, including schools, colleges and universities, have an important role to play in keeping them safe from terrorist propaganda. This paper examines the implementation of the national *Prevent Strategy* in the UK, intended to deter those who encourage others to become terrorists and to stop those being radicalised and drawn to extremist causes.

For more than two decades the UK *Prevent Strategy* has sought to prevent terrorism and its underlying causes, including programmes to prevent radicalisation to extremist causes in schools, colleges and universities. This approach has proved to be controversial and is not without its imperfections. This paper explores how the *Prevent Strategy* is tackling the radicalisation of young adults in schools, colleges and universities, reflecting on the challenges of implementation, and the steps necessary to prevent a very small but increasingly sophisticated minority of violent extremists from recruiting and radicalising children and young adults to their violent ideologies.



1. Introduction – The catalyst for change

At the time of the devastating Al-Qaeda Planes Operation of 9/11 in the United States (US), the United Kingdom (UK) government, like the US and many other countries in the developed world, had no sophisticated nor coherent cross-departmental strategy to counter international terrorism. In short, the UK had no plan to institute of any rigour that would have been able to effectively respond to a major Al-Qaeda indiscriminate attack. The characteristics of violent jihadist terrorism with its vaulting ambitions, strident ideology, and disregard for civilian casualties – with adherents prepared to give their lives in their attacks – represented very new challenges for politicians, government policy-makers, and intelligence and law enforcement agencies alike¹.

In the immediate aftermath of 9/11, the threat from extreme jihadist terrorism in the UK had been assessed as severe, and numerous plots affecting British interests overseas and at home were of great concern to the security authorities. In 2002 policy makers began work on a UK counter-terrorism strategy called **CONTEST: CouNter-TErrorism STRategy**². The strategy was later presented to the British Cabinet and adopted in 2003. The details of the new strategy remained confidential and were not made public by the government until 2006 following the Al-Qaeda inspired coordinated suicide terror attacks on London's public transport system on 7 July 2005. This devastating attack, which killed 52 innocent civilians, proved to be a catalyst for unprecedented change in UK counter-terrorism policy. The London 7/7 terror attack served to amplify the discord between the geographically anchored specialist policing assets and the amorphous threat from distributed non-hierarchical cells affiliated to Al-Qaeda. The terrorist threat appeared to be emerging from all sides, being variously imported into the UK or returning from overseas with individuals having received military training or combat experience in the theatres of conflict in Iraq and Afghanistan. The threat was also coming from within UK borders; the incubation of a home-grown threat had been identified and drawn from the very communities the coun-



ter-terrorism apparatus of the state was attempting to protect. The threat was also virtual with terrorists being recruited, radicalised, trained and tasked online in the ungoverned digital domain of cyber space.

The immediacy and the diversity of the domestic UK terror threat brought about a series of fresh challenges. At the core of many of the changes required to tackle Al-Qaeda inspired terrorism was the problematic shift to the pre-emption or interception of terrorism. This was a shift necessitated by the suicidal component of terrorist tactics, a shift that had far-reaching implications for national security. The policing of political violence – traditionally categorized as intelligence-led and politically sensitive – had historically generated structures which had been remote, secretive and specialist. Yet the contemporary evolution of terrorism had spawned important new trends and demanded a new policing response. Contemporary terrorism now involved embedded citizens as much as foreign extremists. While that phenomenon may not have been new to other parts of the world, it certainly represented a significant change in Britain.

The way in which members of UK communities were being influenced by the extreme single narrative of the religious ideology promoted by Al-Qaeda was of critical concern for the UK Government. This single narrative, when combined with a complex malaise of social and economic factors, served to manipulate individuals towards extremist perspectives cultivating a home-grown terrorist threat. Understanding why British citizens were moving towards extremist perspectives and creating an alternative to allow them to resist such views was widely acknowledged as the key challenge in countering the contemporary terrorist threat. As a direct result, the need for credible and actionable intelligence to monitor and prevent terrorism came to the fore and was added to the more traditional tactic of the pursuit through criminal justice processes. The imperative to refocus and react to new trends was made manifest in the Government's CONTEST strategy to counter international terrorism being structured in what became known as the '4P' campaigns which included: *Pursue*, to stop terrorists attacks; *Prevent*, to stop people becoming terrorists, or supporting



violent extremists; *Protect*, to strengthen protection against terrorist attack; and *Prepare*, where an attack cannot be stopped, to mitigate its impact.' The strategy that emerged from this work had a clear strategic aim to make it possible for society to maintain conditions of normality so that people could go about their normal business, freely and with confidence, even in the face of suicidal terrorist attacks. In developing the *Prevent, Pursue, Protect and Prepare* structure of CONTEST, the strategy was easily understood as a logical narrative, translated into specific programs of action across government, the private sector and the voluntary sector, and as has been shown, capable of being updated and extended in response to developments in the threat. It was important that the complexities of such a wide-ranging strategy were simplified and focused as successful delivery would depend upon a joined-approach and the strength of partnerships. As CONTEST developed, additional focus was concentrated upon the preventative ways in which the early identification of UK home-grown terrorist threat could be developed.

2. Prevent emerges – Putting policy into practice

The '*Prevent*' strand of CONTEST was focused towards tackling the radicalization of individuals. It set out to do this by addressing structural problems in the UK and overseas that may contribute to radicalization, such as inequalities and discrimination. To prevent terrorism and its underlying causes was recognized as requiring a long-term approach. Prevent was intended to deter those who facilitate terrorism and to deter those who encourage others to become terrorists. This required a change in the environment where extremists and those radicalizing others operated. The *Prevent* strand also aimed to engage in the battle of ideas, to win hearts and minds by challenging the ideologies that extremists believe can justify the use of violence. Preventing violent extremism remains a key area of CONTEST and is the proactive element of the strategy. The government believes that the UK, like many other countries, faces a challenge from terrorism and violent extremism where a very small minority seeks to



harm innocent people in the name of an ideology which causes division, hatred, and violence. Within the first publication of CONTEST during July 2006, Prime Minister Tony Blair expressed his concerns about the increasing specter of Al-Qaeda inspired violence stating that: “This terrorism will not be defeated until its ideas, the poison that warps the minds of its adherents, are confronted, head-on, in their essence, at their core³.” The role of the government is to take tough security measures needed to keep people safe but a security response alone was considered insufficient to reduce the terrorist threat. A response led and driven by local communities was however believed to be a vital component to tackle the home-grown Al-Qaeda inspired terrorist threat. The very essence of the *Prevent* pillar of any counter-terrorism strategy seeks to engage partners to work together to challenge and expose the ideology that sanctions and encourages indiscriminate violence. Al-Qaeda inspired terrorists plots in the UK, discovered in the immediate aftermath of 9/11 and which continued after the London 7/7 bombings, supported the pressing need to stop people, especially young people, being drawn into illegal activities associated with violent extremism. *Prevent* therefore prioritized its response, revealing that the government needed to expose and isolate the apologists for violence and protect the places where they operate. The government also revealed that local authorities, the police, and their partners in schools, other educational institutions and elsewhere, have a critical role in preventing violent extremism as they understand the local context. They are in a unique position to talk to local communities, hear their concerns and enable people to stand shoulder to shoulder, confident in their rejection and condemnation of violence.

The *Prevent Strategy* drilled deep into the core of British values, the government revealing that everyone has a right to live in a safe and welcoming neighbourhood where they feel they belong. CONTEST revealed that the government firmly believed that when people have a say in the design and delivery of public services, those services better meet their needs. These set of beliefs presented UK authorities with a real challenge: how to prevent people from adopting extremist perspectives without labelling them,



isolating them or without the authorities distancing themselves from the very communities with whom they wished to engage and who otherwise could help to prevent pockets of extremism from developing. It was also recognised that a robust strategy to prevent violent extremism that leads to terrorism has to navigate and infiltrate a complex environment online and in the real world.

In the UK, concepts such as community involvement, multi-agency working and public assurance – now widely accepted and practised in local policing – had to migrate into the policing of violent extremism. All police officers, and not just those specialist counter-terrorism officers, therefore

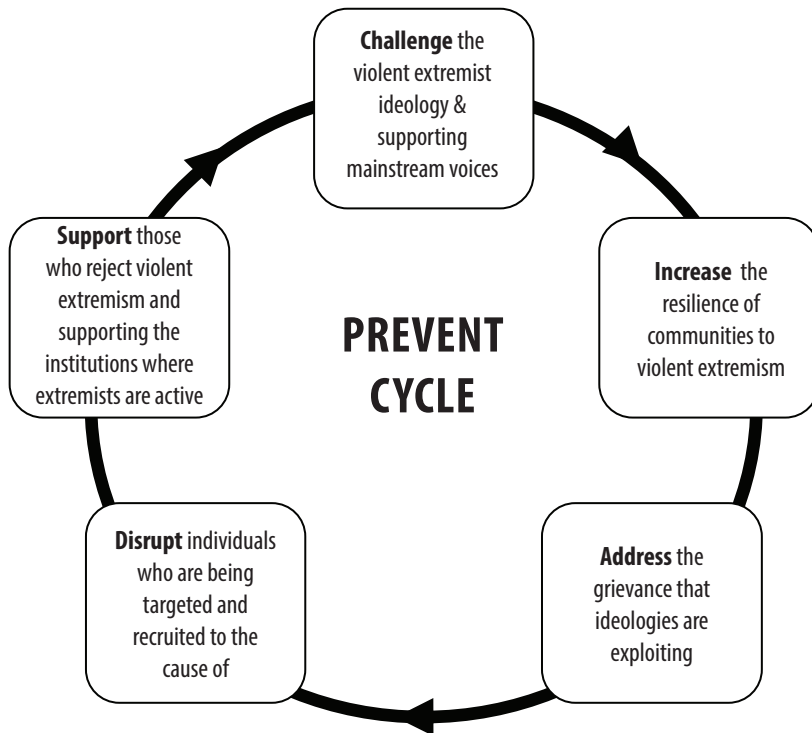


Figure 1 – The Prevent Cycle



had to share in the tasks given the scale and scope of the terror threat from home-grown radicalized extremists. Counter terrorism policing thus became a matter for all in the police, for all their strategic partners and for all the public.

The *Prevent Strategy* highlighted that everyone has a right to live in a safe and welcoming neighborhood where they feel they belong. At the same time, it identified that no neighborhood can truly succeed unless local people define their future by working together to tackle the challenges they face. Moreover, to prevent terrorism at its source required a cycle of sustained effort illustrated in *Figure 1 – The Prevent cycle*, which includes challenging violent extremist ideology and supporting mainstream voices, increasing resilience of communities, addressing the grievance that violent ideologies are exploiting, disrupting those who are being targeted and recruited to violent extremist causes, and supporting them and institutions to reject extremist ideologies.

The long-term solution to preventing terrorism is to stop people becoming terrorists or becoming involved in violent extremism. Through the UK Governments *Prevent Strategy*, the police service and its partners have an integral role to play working with local communities to support people who are vulnerable to being drawn into criminal activity and to challenge those who support violent extremism. Supporting those who may be vulnerable to being drawn into violent extremism is a key strand of the UK Governments *Prevent Strategy*. To be effective this approach depends upon the creation and maintenance of a partnership approach requiring the acceptance of a shared responsibility and active participation, an approach which continues to be tested by the radicalization and recruitment of young people to violent, extreme and terrorist causes.



3. Radicalization and recruitment – Preventing teenage terror plots

In June of 2006, Hammad Munshi, a 16 year old schoolboy from Leeds in the North East of England, was arrested and charged on suspicion of committing terrorism related offences. Following his arrest, police searches were conducted at his family home where his wallet was recovered from his bedroom⁴. It was found to contain hand-written dimensions of a sub-machine gun. Munshi had excellent information technology skills and had registered and ran his own website on which he sold knives and extremist material.

He passed on, for example, information on how to make Napalm as well as how to make detonators for Improvised Explosive Devices (IED). At the time of his arrest Munshi had been directly influenced by being exposed to extremist rhetoric and propaganda on the internet unbeknown to his family, friends and wider social network. At the time of his actual offending Munshi was just 15 years of age and was radicalised to the violent jihadist ideology of Islamic State but it was not only this extremist doctrine that was recruiting teenage boys to radical causes. On 20th September 2019 at Leeds Crown Court, a boy who tried to build a bomb at the age of 15 was convicted of terrorism offences and jailed for five years. Kieran Cleary had researched extreme right-wing and anti-Muslim material online and had praised Adolf Hitler during his radicalisation journey. The sentencing of Cleary followed an announcement by the UK's most senior counter-terrorism police officer, Assistant Commissioner Neil Basu of the Metropolitan Police, who warned that right-wing extremism posed the fastest growing terror threat to the UK.

During a presentation to journalists, Mr Basu revealed that around 10 per cent of 800 live counter-terror investigations in the UK involved far-right extremists – a significant increase on previous years. Mr Basu also warned that teenagers were increasingly being drawn into far-right extremism. When UK anti-terror police arrested Cleary and searched his



home in August 2018, they found a shrapnel-filled device that could have been made into a viable CO2 bomb. The court heard that the teenager had researched bomb-making tactics on the dark web and almost created a weapon with a 30 metre blast radius that would have caused maximum harm and death to civilians. The Crown Prosecutors explained to the court that Cleary told friends he was going to “go on a rampage” and “kill many people” weeks after making the device. The jury heard that Cleary first came to the police’s attention aged 13 and was referred to the UK’s Prevent counter-extremism scheme for support and intervention but efforts to intervene could not stop him developing his extremist views into terrorist acts. Detective Chief Superintendent Martin Snowden, the head of Counter Terrorism Policing North East, revealed that Cleary had spent a lot of time alone on the internet in this disturbing case stating: “His fascination with violence and death is particularly concerning given his age and vulnerability. Despite extensive attempts to steer this boy away from the path of criminality, due to the progression of his behaviour, he was arrested and charged with serious offences. His online searches combined with the manufacture of an explosive device had the potential to put the safety of others at risk and could not go unprosecuted.”⁵

The case of Cleary brought into sharp focus the vulnerability of young teenagers of school age to the extremist online propaganda but Cleary was not the youngest teenager to be arrested and charged with terrorism-related offences in the UK. At just 14-years-old, a schoolboy from Darlington in the UK became one of the youngest people in the UK to be convicted of terror charges. The boy, who cannot be named because of his age, appeared before Westminster magistrates court in 2022 charged with possessing a terrorist publication. He pleaded guilty to three offences contrary to section 58 of the Terrorism Act 2000, admitting possessing a record of information likely to be useful to a person committing or preparing an act of terrorism.⁶ Police said the charges related to extreme right-wing terrorism. The teenage terror trend is not unique to the UK, many nations across the world have seen an increase of the young and impressionable being coerced into planning and committing acts of violence. In Aus-



tria during 2025, the foiled teenage terror plot to slaughter Taylor Swift fans attending the Era's Tour concert in Vienna provided further evidence that the recurrent targeting of crowded public spaces by teenage terrorists – radicalised and recruited by the outlawed Islamic State (ISIS) terrorist group – remains a significant threat. The cancelling of the concert was a victory for violent extremists operating across Europe who are actively being encouraged by online propaganda to exploit the intrinsic vulnerabilities of what are considered “soft targets”, such as stadiums and concert halls, a term that derives from their open nature and public character.

The arrest of three teenagers by security forces in Austria revealed their attack plans which appears to have sought to combine the use of homemade explosives with marauding knife attacks with the intent of causing mass casualties as fans made their way to the concert venue.⁷ Following their arrest, Vladimir Vorokov, the United Nations Under Secretary for Counter Terrorism, revealed that Europe faces a more acute threat from Islamic State Khorasan Province (ISIS-K), the ISIS affiliate to whom a 19-year old man pledged allegiance before plotting to terrorise Taylor Swift's concertgoers in Vienna. Vladimir Vorokov stated: “ISIS mostly operates through branches in different parts of the world, and the one that I would say is the most successful, and arguably the only one that has been consistently operating also in the West and planning terrorist attacks in the West, is ISIS-K. This group is considered the greatest external terrorist threat to the continent”.⁸

The continued rise of teenagers being indoctrinated by terrorist ideologies in the UK and across Europe continues to raise concerns about how the police and their network of partners can better develop ways in which to identify the early signs and indicators of radicalisation development to prevent teenagers being drawn to terrorist causes.



4. Play your part - Educating against extremism

The education sector has an important role to play in preventing violent extremism. We must first, however, face an uncomfortable truth; some terrorist organizations operating today have recruited children to their cause. All in authority must now recognize that terrorists operating in the UK, and across Europe, are intentionally and systematically targeting young people, and individuals as young as 13 and 14 have already been implicated in terrorist-related activity. In the UK, most of the teenagers arrested for terrorism related offences have been educated in British schools and several have exhibited degrees of vulnerability while of school age prior to being radicalized as teenagers. The purpose of the *Prevent Strategy* in schools is simply to offer opportunities to help young people understand the risks associated with violent extremism and to develop knowledge and skills to be able to challenge extremist arguments. Preventing violent extremism from emerging within young people in schools supports the *Prevent Cycle* by:

- Using teaching and learning to help young people develop the knowledge and skills to challenge extremist narratives.
- Identifying how to prevent harm to pupils by individuals, groups or others who promote violent extremism.
- Providing programmes to support pupils who are vulnerable.
- Increasing the resilience of pupils and school communities through the curriculum, other learning opportunities or activities.
- Using teaching styles and curriculum opportunities which allow grievances to be aired.

Accepting that the potential radicalization of young people of school age is an issue to be addressed is the first and most important step in countering this threat. It cannot and must not be ignored, yet preventative measures in schools requires a sensitive, delicate and morally justified response—but it does require a response. It is widely acknowledged across



government, in particular departments responsible for schools, education, children and families, that preventing violent extremism in schools is a challenging issue which needs to be a shared endeavour across local partners and communities, with activities tailored to meet local needs. Young people represent the future of society which educates them to identify a variety of risks such as alcohol, tobacco, vaping, drugs, and gambling, it is also important to support the welfare of pupils who may be particularly vulnerable to recruitment and radicalization. *Prevent* in schools serves to highlight the complexity of the threat of today's terrorism and the reach required of counter measures to protect the public now and in the future.

Universities and colleges also have an important role to play in preventing terrorism. They hold a unique cultural and legal position in the UK and provide a complete learning experience through a mix of social and academic opportunities. There are times, however, when universities need support from other agencies to safeguard the well-being of their students. In 2008, the Centre for Social Cohesion Commission published the results of their in-depth and groundbreaking study into attitudes towards Islam on British university campuses.

Still the most comprehensive study to date, the research discovered, among other things, that students who are active in their university Islamic society were twice as likely as non-members to hold extreme views, including that killing in the name of religion being justified. Studies also show that more than 30% of people convicted of Al-Qaeda associated terrorist offences in the UK between 1999 and 2009 were known to have attended university.⁹ A report of research findings published during 2010 by the Centre for Social Cohesion *Radical Islam on UK Campuses - A Comprehensive List of Extremist Speakers at UK Universities*, found that a significant number of students and graduates from UK universities have committed acts of terrorism or have been convicted for terrorism related offences, in the UK and abroad.¹⁰ The report also revealed that more than 30.71% of individuals involved in violent Islamist terrorism in the UK were educated to degree level or higher. Of these, 19 individuals studied at



a UK university; 16 were graduates; three were postgraduate students and one had achieved a postgraduate qualification. A further finding of the research identified that at least four individuals involved in acts of terrorism in the UK were members of their student's union Islamic society, and a further six were studying at a UK university at the time of their arrest. In a number of terrorism cases both in the UK and worldwide, the individuals involved were reportedly radicalised on UK university campuses.

While the body of evidence gathered by the Centre for Social Cohesion strongly suggests that the radicalisation of young adults while studying at university presents a risk, this does not in any way mean that higher education institutes are at fault for the development of radicalisation. With a large and diverse student population attending university, some extremist organizations target specific institutions with the objective of radicalizing and recruiting students. As a direct result of this emerging threat the *Prevent Strategy* stated that further and higher education institutes have a role to play in reducing the risk from terrorism by working in partnership to challenge terrorist ideologies, support those who are vulnerable to being radicalized, and work with those institutions where radicalization takes place. To build effective partnerships between police, colleges and universities, police officers should use the '4R' model for reducing risk of radicalization at universities shown in *Figure 2*, including the key elements of the process concerning *Risk*, *Responsibility*, *Relationships* and *Referral*.

It is important for the effective delivery of the Prevent Strategy that police officers engaging with colleges and universities acknowledged that they must uphold academic freedom and provide an environment for research and open debate but in this context all in authority within education institutes must acknowledge the following;

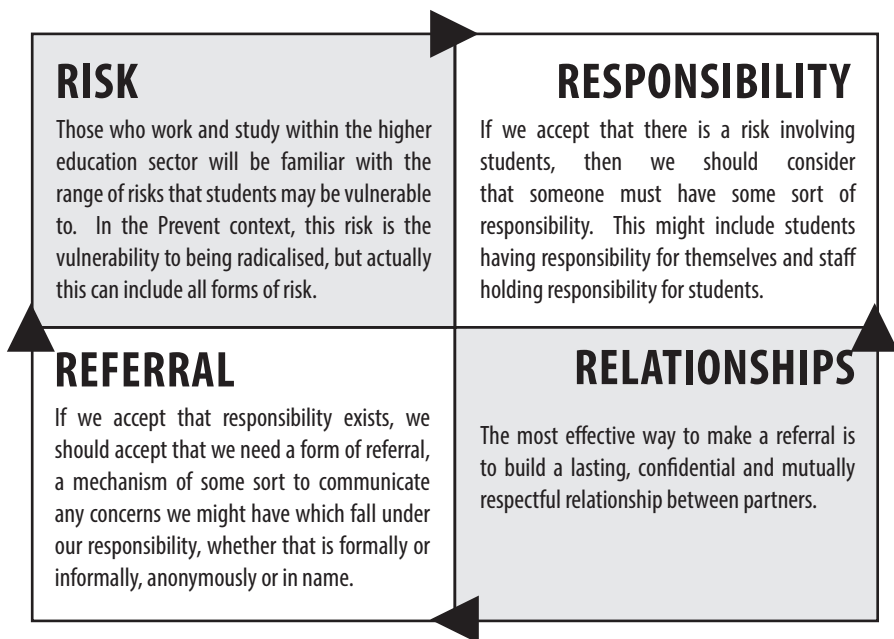


Figure 2 – 4R Prevent Model: Reducing the risk of radicalization in universities

- Colleges and universities possess some form of risk for their students and staff;
- College and university staff, students and the police have a responsibility to help minimize and mitigate against the risks to public safety;
- College, university, and police information sharing and referral mechanisms are crucial;
- College, university, and police collaborative partnerships and relationship building form the foundation of future work to identify, mitigating, minimize and manage risk to public safety



These themes assist in creating the simple ‘4R’ model for reducing risk at universities. Police officers who work with colleges and universities may find the model useful in discussing how *Prevent* fits with students and staff. The positive outcome of the model is that risk is reduced by building strong professional relationships. The use of the 4R model as a basic tool to build partnerships between the police service and universities is an effective framework to explain how information sharing and raising awareness of vulnerability can be understood by those who work within universities. It provides a basis on which to build a positive and productive working relationship. In practice, building long-term strategic partnerships means that police, college and university colleagues must get to know one another, share information appropriately and work together to solve challenges. From police *Prevent Strategy* perspectives, this relationship is not about gathering intelligence, it is talking about the risks of racialization and working together to manage, mitigate and minimize the risks to public safety by providing support to vulnerable citizens as part of safeguarding the young and vulnerable in society.

To reinforce the importance of preventing terrorism by police and all partners, the UK government introduced the Prevent statutory duty through the Counter-Terrorism and Security Act 2015.¹¹ The duty requires local authorities, schools, colleges, higher education institutions, as well as health bodies, prisons and probation, and the police, to consider the need to safeguard people from being drawn into terrorism. It sits alongside long-established duties on professionals to safeguard vulnerable people from exploitation from a range of other harms. This *Prevent Duty* shrines into UK law the role and responsibility of all institutions to protect those vulnerable to radicalisation. The *Prevent Duty* also provides mechanisms and frameworks to support authorities and institutions to fulfil their *Prevent Duty*, including the introduction in all areas of the UK of the requirement to have local action plans in place to support vulnerable individuals; in some areas this support is provided by a process known as *Channel*. *Channel* provides a mechanism for supporting those who may be vulnerable to violent extremism by assessing the nature and the ex-



tent of the potential risk and, where necessary, providing an appropriate support package tailored to an individual's needs.¹² A multi-agency panel decides on the most appropriate action to support individuals taking their circumstances into account. The partnership focused structure is similar to existing, successful partnership initiatives which aim to support individuals and protect them from harm, such as drugs and involvement in knife crime and gang culture.

Supporting those most at risk of being drawn into violent extremism is about diverting people away from potential risk at an early stage which prevents them from being drawn into criminal activity. Partnership involvement ensures that those at risk have access to a wide range of support ranging from diversionary activities through to providing access to specific services such as education, housing and employment. Partners may include, depending on local circumstances: education, health, probation, prisons, police, social services, children's and youth services, border agencies, voluntary services, charitable organisations and community members. *Channel* is not about reporting or informing on individuals in order to prosecute them. It is about communities working together to support vulnerable people at an early stage, preventing them from being drawn in to violent extremism. There are currently 28 local coordinators across more than 70 local authorities.

Those in communities who have concerns about individuals who may be vulnerable are advised to contact their local authority, the police or other trusted local organization for further advice. The critical success factors of the *Prevent Strategy* in schools, colleges and universities is the sharing of experiences and challenges, the development of partnerships, and the creation of a platform from which to engage and raise awareness of the threat from terrorism and violent extremism to ensure communities are safer and feel safer. Despite the best efforts of all *Prevent Strategy* partners and the statutory *Prevent Duty* being in place, serious problems persist.

The latest UK Government Home Office figures, released in 2025, reveal that 8,778 individuals were referred to the *Prevent Strategy* programme



between April 2024 and March 2025, which is the highest number since records began in 2015.¹³ This represents a 27 per cent increase compared with the previous year and reflects growing concerns around radicalisation and safeguarding. This release of data contains official statistics in development on individuals referred to and supported through the *Prevent Programme* due to concerns they were susceptible to radicalisation. Following initial screening and assessment, referrals may be passed to a multi-agency Channel panel where a risk of radicalisation exists. In 2025, the Home Office Prevent Programme figures reveal that the education sector made the most referrals (3,129; 36%), followed by the police (2,631; 30%).

These figures highlight the vital role that teachers play in ensuring that individuals vulnerable to radicalisation receive early support, as most referrals are for 11- to 15-year-olds, with 36 per cent of all referrals (where the age is known) being for this age group in 2024-25. The second largest proportion of referrals in the past year was for those aged 16 to 17 (13 per cent). Overall, the referral data reinforces the critical role that the education sector plays in identifying early signs of radicalisation. It also points to the need for multi-agency collaboration, particularly where there is crossover with mental health and special educational needs and disabilities.

The key takeaway from the recent set of published *Prevent Programme* data from the Home Office is that multi-agency collaboration between partners is essential for preventative safeguarding measures to succeed and to overcome the problems of delivering *Prevent Strategy* policy.

5. Lessons to be learned – Problems with Prevent

The UK, like many other nations across the world, faces a real and sustained threat from terrorism and violent extremism. Tough security measures are needed to keep communities safe but a preventative response led and driven by local partners is also vital. The *Prevent Strategy* has been established as a response to this longer-term challenge because



violent extremists are constantly seeking to exploit new tactics and technologies in both attack planning and recruitment. The *Prevent Strategy* therefore enables the police service to adapt and strengthen its response to deter people joining the recruitment line. The police service is gaining a better understanding of the communities they serve as a direct result of implementing the *Prevent Strategy* and are engaging more actively with hitherto hard to reach communities and working more closely with key partners — all of these are key to building an atmosphere of trust rather than grievance and resentment. Delivering the *Prevent Strategy* is without doubt a challenging and complex arena that requires a whole community approach to empower communities, challenge those who espouse violence and support those who are vulnerable to being drawn into violent extremism. It will only have effect if the police service continues to build trust and confidence through renewed and consistent engagement activity.

The police service responsibility to deliver the *Prevent Strategy* is not a short-term priority to be discontinued as the threat level recedes. The threat from terrorism remains high in the UK and it is vital that the policing response remains dynamic in response to violent extremism from wherever it emerges. The *Prevent Strategy* is something that the police service is doing with its partners and all communities with a longer-term objective. It is a shared objective that most importantly, brings the police service closer to the communities they serve and protect.

The early efforts and initial approaches by the UK government to implement preventative counter terrorism action through the *CONTEST Strategy* was by no means welcomed and supported by all. Many in society held the view that the government response through the *Prevent Strategy*, and being driven by the police, was a knee-jerk reaction which failed to create a coordinated, comprehensive policy to tackle the post London 7/7 terrorist threat. Those individuals who were opposed to the initial *Prevent Strategy* suggested that that it played to the emotions of the general public for the government and the police to be seen to be tough on terrorism and the causes of terrorism as aroused by the media and national press.



Many ethnic minority communities also felt that the *Prevent Strategy* representing government policy was being solely directed at their religion. In developing the *Prevent Strategy*, aspects of counter-terrorism policy at a local community level positioned the government and the police service in uncharted territory. Never before had national central government counter-terrorism policy been directly linked to local community issues in this way. Allegations of spying on communities and criminalising entire communities as being either terrorists, potential terrorists, or potential future terrorists, due to their faith and ideology, were levelled at government and the police. Yet despite strong views opposing the government's preventative approach, the challenge of protecting the young and vulnerable in society from recruitment and radicalisation of violent extremists had to be tackled.

For the police service, community engagement is quite properly an important part of the *Prevent Strategy* which serves as a response to the wider challenge of tackling contemporary terrorism and violent extremism. But inevitably there will continue to be times when police intelligence-based activity, targeted at specific terrorist suspects within communities, will rub up uncomfortably against *Prevent Strategy* initiatives to engage with the community more broadly. This is likely to be a recurring theme in counter-terrorist work in the UK in the years ahead. The police service and its partners will need to continue to invest effort in explaining their actions to ensure that they retain public confidence. But it cannot and must not be allowed to deflect the police service and its partners from continuing the intelligence work which is necessary and proportionate to match the terrorist threat. As the *Prevent Strategy* has matured, it has increasingly recognized the many forms of violent extremism to be addressed in Britain today, and not just those linked to the original aim of the *CONTEST Strategy* in tackling the Al-Qaeda genre of international terrorism. Ensuring that strategies for intervention were targeted towards those most vulnerable in UK society was pivotal to the long term success of preventing violent extremism in all of its forms. The key challenges in leading the *Prevent Strategy* for the police service have been winning



and sustaining support from local authorities and other partners. *Prevent Strategy* challenges have included facing the accusations of unfair targeting of, or worse, spying upon Muslim communities.

The *Prevent Strategy* is also not wholly accepted by universities or students; despite the strategies aim to support those who are vulnerable from becoming terrorists. The UK's National Union of Students finds the language and approach of the *Prevent Strategy* problematic, whilst academics are concerned at the potential erosion of freedom of speech. It is important that the police should not expect students or staff to readily accept the *Prevent Strategy* and its approach. In fact, if police who engaged with colleges and universities embrace challenge and debate whilst being aware of the sensitivities that students and academics might possess, the *Prevent Strategy* has a much greater chance of success. Many political and academic commentators continue to argue that the *Prevent Strategy* is flawed, confusing the delivery of Government policy to promote integration with Government policy to prevent terrorism. Moreover, commentators arguing against the *Prevent Strategy* suggest that it is failing to confront the extremist ideology at the heart of the threat the UK faces. Yet, despite these accusations, the *Prevent Strategy* has endured, being independently reviewed and updated at regular intervals by successive UK governments.

6. From threat to threat – The future of Prevent policy

While the UK has rightly made strides towards an increasingly open and public facing domestic security apparatus, the very nature of counter-terrorism remains enshrined in a preventative ethos. To prevent terrorism and to render visible what others do not want us to know, counter-terrorism must be intelligence-led and so necessitates a covert approach. That being said, not all counter-measures need to be cloaked in secrecy for them to be effective, and the contemporary phase of counter-terrorism has evolved important new trends alongside palpable moves towards expansion and localism. Countering terrorism today is a collaborative ap-



proach. No one single government agency or department can protect its nation from the diverse range of terrorist threats endured at home and overseas. To ensure a holistic response, all in authority must now bring their expertise to bear in concert with one another in the nation's interest, which includes intelligence agencies, police, schools, parents, and wider society, to prevent the development of extremist views that may lead to violence and acts of terror. Preventing terrorism and violent extremism remains the most challenging aspect of countering terrorism in all of its forms. Methods to prevent terrorism have proved controversial and are not without their imperfections. The UK's *Prevent Strategy* has been continuously developed and updated from its original iteration devised in the aftermath of the 9/11 terrorist attacks in the US. Despite this sustained effort of prevention terrorist groups have radicalised and recruited young people, to their causes, a problem that continues to persist.

The learning from implementing the *Prevent Strategy* in Britain over the last two decades is that all preventative measures, whether programmes for schools, colleges, universities, probation services, prisons, or for the wider general public, requires a shared, sensitive, delicate and morally justified response, and one that is underpinned through continuous monitoring mechanisms to ensure that the response remains appropriate and proportionate to tackle complex terror threats to both neighbourhood safety and national security. Recognising that the potential radicalisation of young people of school age in modern society is a safeguarding issue to be addressed is the first and most important step all in authority must take to counter this persistence menace – it cannot and must not be ignored – and all schools, colleges and universities are encouraged to protect the children and young adults in their care from adopting extremism and violent ideologies that may lead to terrorism.



-
- 1 Staniforth, A The Routledge Companion to UK Counter-Terrorism. (2012) Oxford: Routledge (ISBN 9780415685856) Available online: <https://www.routledge.com/The-Routledge-Companion-to-UK-Counter-Terrorism/Staniforth-Sampson/p/book/9780415685856> (Accessed 25 January 2026)
 - 2 HM Government Counter Terrorism Strategy (CONTEST), (2023) Available online: <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023> (Accessed 24 February 2026)
 - 3 Staniforth, A The Routledge Companion to UK Counter-Terrorism. (2012) Oxford: Routledge (ISBN 9780415685856) Available online: <https://www.routledge.com/The-Routledge-Companion-to-UK-Counter-Terrorism/Staniforth-Sampson/p/book/9780415685856> (Accessed 25 January 2026)
 - 4 Staniforth, A Teenage terror: How do we educate the young against extremism? (7 October 2019) Policing Insight Available online: <https://policinginsight.com/feature/opinion/teenage-terror-how-do-we-educate-the-young-against-extremism/> (Accessed 25 February 2026)
 - 5 Staniforth, A Teenage terror: How do we educate the young against extremism? (7 October 2019) Policing Insight Available online: <https://policinginsight.com/feature/opinion/teenage-terror-how-do-we-educate-the-young-against-extremism/> (Accessed 25 February 2026)
 - 6 HM Crown Prosecution Service <https://www.cps.gov.uk/types-crime/terrorism#:~:text=Section%2058%20makes%20it%20an,containing%20information%20of%20that%20kind.>
 - 7 The Independent Taylor Swift Vienna plot arrest (9 August 2024) Available online: <https://www.independent.co.uk/news/uk/home-news/taylor-swift-vienna-terror-plot-arrest-b2593822.html> (Accessed 2 February 2026)
 - 8 ABC News After Taylor Swift concert plot, UN official calls ISIS-K 'greatest' external terrorist threat to Europe (9 August 2024) Available online: <https://abcnews.com/Politics/isis-greatest-external-terrorist-threat-europe-amid-foiled/story?id=112690609> Available online: (Accessed 15 February 2026)
 - 9 The Guardian Radical Islam gains ground in campuses (27 July 2008) Available online: <https://www.theguardian.com/world/2008/jul/27/islam.highereducation> (Accessed 18 February 2026)
 - 10 The Centre for Social Cohesion Radical Islam on UK Campuses - A Comprehensive List of Extremist Speakers at UK Universities (2010) Available online: <https://henryjacksonsociety.org/wp-content/uploads/2013/01/RADICAL-ISLAM-ON-CMAPUS.pdf> (Accessed 23 February 2026)
 - 11 HM Government Prevent Duty Guidance: Guidance for Specified Authorities in England and Wales (2023) Available online: https://assets.publishing.service.gov.uk/media/65e5a5bd3f69457ff1035fe2/14.258_HO_Prevent+Duty+Guidance_v5d_Final_Web_1_.pdf (Accessed 23 February 2026)
 - 12 HM Government Channel and Prevent Multi-Agency Panel (PMAP) Guidance (2026) Available online: <https://www.gov.uk/government/publications/channel-and-prevent-multi-agency-panel-pmap-guidance> (Accessed 21 February 2026)
 - 13 HM Government Prevent Programme Referrals - April 2024-March 2025 (2025) Available online: <https://www.gov.uk/government/statistics/individuals-referred-to-prevent-to-march-2025/individuals-referred-to-and-supported-through-the-prevent-programme-april-2024-to-march-2025> (Accessed 12 February 2026)



PREVENTION BEFORE REPRESSION: HOW POLICE–COMMUNITY COLLABORATION ENHANCES PUBLIC SAFETY AND SECURITY

Ruža Karlović



Summary

This paper proposes a governance approach in which prevention is embedded as a measurable core function of modern policing systems, aligned with, rather than opposed to, enforcement. Modern policing requires the strategic integration of prevention and enforcement, treating them as complementary rather than competing priorities. While enforcement is essential for managing immediate threats, many contemporary security challenges - such as radicalization, violence, and hybrid risks - develop gradually through complex social and digital dynamics. Relying predominantly on a reactive model that intervenes only at the most disruptive stage limits long-term effectiveness and increases both institutional and social costs.

Therefore, prevention must be structurally embedded within policing systems and not treated as a secondary or symbolic activity. When institutionalized through community collaboration, intelligence-led analysis, and multi-sector cooperation, prevention becomes an operational function that strengthens early risk identification and proportionate intervention. Importantly, sustainability does not require new funding streams; it requires the explicit integration of preventive objectives into existing resource allocation, not always more money, staffing models, operational planning, and performance frameworks.

Since preventive success is often reflected in risks that do not escalate, it tends to remain institutionally invisible. To address this issue, evaluation systems should combine activity-based indicators - such as multi-agency coordination and safeguarding efforts - with outcome measures, including reductions in repeat incidents, stabilization trends, de-escalation outcomes, and levels of community trust. By formally recognising prevented escalation as a measurable achievement, police organisations can value prevention alongside enforcement without reducing it to simplistic output statistics. Continuous professional education is also critical. By embedding competencies in communication, safeguarding, early risk identi-



fication, and analytical reasoning into training programs, we ensure that prevention becomes not merely a policy directive but an ingrained professional mindset across all organizational levels. A structured sequencing of prevention and enforcement, supported by measurable indicators and aligned resource planning, offers a practical governance model. This approach enhances public safety, reduces long-term reliance on coercive measures, strengthens legitimacy, and increases institutional resilience in today's risk-oriented societies. The strategic question is no longer whether prevention matters, but whether policing systems (people who are currently in the position of decision-making for recognising prevention as important as classical police work) are designed to prioritise, measure, and allocate resources to it effectively.

1. The Importance of Prioritising Prevention Over Repression

1.1. Why Prevention Must Precede Repression?

Strong enforcement is important for keeping the public safe, especially during serious threats or crimes. However, many risks today, like radicalisation and related violence, grow slowly. They are shaped by feelings of injustice, identity issues, social isolation, and exposure to extreme ideas (Moghaddam, 2005; Borum, 2011). Policing that only steps in when a crime occurs often addresses symptoms rather than root causes. This can lead to a sense of injustice, increase division in society, and weaken community cooperation. Focusing on prevention does not reduce accountability or replace the need for enforcement. Instead, it aims to act earlier, before crimes occur. This helps prevent escalation while maintaining fairness and legitimacy. Concerns that preventive strategies divert resources from essential policing ignore evidence that early intervention can reduce repeat incidents, improve the quality of intelligence, and reduce the long-term need for reactive responses.

A prevention-first approach to policing is not a step back from authority. It



is a strategic change. Enforcement is still crucial, but it works better when combined with early risk identification, appropriate responses, and strong partnerships between police and the community. Removing offenders at later stages without addressing the earlier underlying conditions leads to only limited long-term effectiveness. Reactive approaches may also have unintended negative consequences, including:

- Reinforcing perceptions of injustice
- Increasing social polarisation
- Reducing information
- Sharing within communities

Therefore, prevention should not be viewed as a “soft” alternative to enforcement. Instead, it is a strategic approach that:

- Identifies risks more effectively and earlier
- Applies proportionate responses
- Strengthens legitimacy
- Simplifies the ongoing enforcement process, reducing the workload over time.

2. Enhancing Our Capacity for Prevention

2.1 Legitimacy and Cooperation

Research consistently demonstrates that perceptions of fairness and legitimacy promote public cooperation (Sunshine & Tyler, 2003; Tyler, 2006; Cram, 2024). When communities view the police as procedurally just, they are more willing to share early warning signs and comply voluntarily with law enforcement. Thus, legitimacy serves as an important preventive asset. Research shows that when people believe that the police are fair and trustworthy, they are more likely to report problems in their neighbor-



hoods over time. This means that how citizens view the police can significantly influence their willingness to cooperate and share information with law enforcement (Kuen, 2024).

2.2 Community Policing and Intelligence Integration

Community-oriented policing enhances local knowledge and fosters trust within the community. However, its effectiveness relies more on institutional support than on informal goodwill (Gill et al., 2014). When community policing is integrated with intelligence-led policing:

- Community engagement generates contextual information.
- Analytical capacity aids in risk assessment.

Preventive interventions become more targeted and proportionate (Bullcock, 2013; Carter & Fox, 2019). Community-oriented policing focuses on building connections and trust within neighborhoods. Research shows that its success depends more on how well it's integrated into official practices than on individuals' good intentions (Braga & Weisburd, 2022; Telep & Weisburd, 2019). When intelligence-led policing strategies are paired with organised community involvement, they can lead to better information gathering and a deeper understanding of local issues. This combination enhances the ability to prevent crime (Ratcliffe, 2022).

2.3 Radicalisation as a Social Process

Radicalisation should not be oversimplified to ideology alone. It encompasses:

- Push factors (such as grievances and marginalisation)
- Pull factors (including the desire for group belonging and status)
- Individual vulnerabilities (Borum, 2011).

Simulation models indicate that early contextual interventions are more sustainable than repeated late-stage removals (Pepys, Bowles, & Bouhana, 2020).



3. European Normative Approach

European security governance has evolved from a reactive approach to counterterrorism to a more proactive model focused on prevention. The EU Counter-Terrorism Strategy, established in 2005, marked this change with its four-pillar framework: Prevent, Protect, Pursue, Respond. This framework recognises that threats like violent extremism develop gradually, rather than appearing suddenly. More recent frameworks, such as the EU Security Union Strategy for 2020–2025, reinforce important principles like early risk identification, cooperation between agencies, building resilience, and taking balanced actions.

These principles are based on evidence that security threats arise from complex social, psychological, and digital factors before they lead to criminal acts. The EU policies make a clear distinction between radical opinions and actual violence, which helps protect people's rights and warns against excessive criminalisation—something that could worsen grievances and weaken public trust. The European Code of Police Ethics from 2001 supports this approach, emphasising the need for proportionality and public backing in effective policing.

Legitimacy isn't just an afterthought, it is essential because it fosters cooperation, improves communication, and boosts preventive efforts. Across Europe, community-oriented policing models are not only about visibility and engagement but are explicitly described as part of crime prevention strategies, where police officers work beyond reactive enforcement to proactively reduce crime and improve local safety and security (Bayerl et al. (2017)). The EU Knowledge Hub on the Prevention of Radicalisation promotes the sharing of prevention expertise across sectors at the European level. These instances show a common theme: structured prevention works best when there is clear organisation, assigned roles, proper training, and measurable success. The main argument here is that prevention should come before repression in modern democratic policing. While enforcement is necessary for addressing immediate threats, a heavy reliance



on reactive measures can be disruptive and costly. Prevention aims to strengthen security, not by replacing enforcement but by minimising the need for coercive actions and encouraging earlier, appropriate responses. To implement this prevention-first approach effectively, local contexts must be considered. The way this strategy is put into practice will differ based on: social cohesion and trust within the community, crime patterns and trends, the digital environment for threat, existing collaborations among agencies, legal and accountability frameworks etc.

At the local level, applying the principle of Prevention Before Repression requires three key changes:

- Integration into Police Work
- Prevention should be incorporated into everyday planning, staffing, and evaluation in police stations rather than treated as an afterthought.
- Collaboration Across Agencies
- Police need to connect with schools, social services, and civil society organisations, especially to support early intervention and help reintegrate individuals.
- Police resources should be allocated to allow time for early engagement and problem-solving while remaining prepared for necessary enforcement actions.

In summary, while prevention is a fundamental goal for security, it is essential to tailor its design to fit local circumstances. The underlying strategy remains consistent: fostering early detection, implementing appropriate responses, and encouraging cooperation can lead to more effective long-term safety outcomes than waiting for issues to escalate before enforcing the law. Thus, embracing the concept of “Prevention Before Repression” is not only an ideal to strive for but also a practical approach. When customised to reflect local realities, it significantly enhances security and supports democratic values.



4. Advancing Prevention: A Collaborative Model for Station-Level Operations

Effective prevention requires more than informal community engagement or reactive enforcement. It requires a structured station-level model that clearly distinguishes intelligence functions and aligns them with community policing objectives. Agencies developing Intelligence-Led Policing (ILP) capacity should establish formal information-sharing systems, analytical products, and dedicated communication channels rather than attaching intelligence tasks to existing community policing structures without strategic clarity (Fox, 2018). A conceptual distinction between Community-Oriented Policing (COP) and ILP enhances effectiveness: community policing strengthens local legitimacy and information flow, while ILP structures and analyses that information to guide prioritisation and intervention.

To operationalise prevention, each police station should embed a Community/Prevention Cell consisting of a team lead and designated prevention officers with territorial accountability. Core functions include regular community contact, identification of local priority risks, early recognition of escalation, safeguarding referrals, and structured multi-agency coordination. Digital prevention functions should complement, not replace, community engagement and remain clearly separated from investigative cybercrime.

Training forms the institutional backbone of this model. Officers require competencies in communication, de-escalation, cultural awareness, radicalisation processes, and safeguarding pathways, while leadership must be equipped to manage multi-agency cases, conduct evaluations, and implement digital prevention strategies (CEPOL, 2021). Prevention must also be measurable. Quarterly monitoring should track partnership activity, community trust indicators, repeat incident trends at micro-locations, safeguarding referrals, de-escalation outcomes, and digital engagement metrics (Sherman, 2013; Hinkle et al., 2020). This model does not eliminate enforcement; rather, it changes our approach to it. Focusing on prevention before enforcement is a more effective strategy. This involves in-



tegrating early intervention, thorough analysis, and teamwork into police station operations. When prevention is built into the system, monitored, and adequately funded, it reduces the need for forceful actions over time. Additionally, it enhances public safety and strengthens trust in democratic processes. Prevention serves as both a strategy and a tactic. Emphasising the micro level is crucial, as radicalisation and crime are always linked to specific local contexts.

5. Monitoring and Evaluation

To enhance crime prevention efforts, police agencies should adopt a structured monitoring framework that goes beyond verbal commitments. Evidence-based policing research shows that systematic assessments are crucial for effective and sustainable preventive strategies (Sherman, 2013; Hinkle et al., 2020). Measurable prevention is key to achieving real results. Quarterly evaluations can focus on clear indicators, including the quality of partnerships with community stakeholders, community trust surveys on perceptions of procedural fairness (Jackson et al., 2012), trends in repeat incidents at crime hotspots (Weisburd, 2015), safeguarding referrals for at-risk individuals, documented de-escalation outcomes (Engel et al., 2020), and the effectiveness of digital engagement strategies (European Commission, 2020). Additionally, continuous investment in education and professional development is essential. Ongoing training for all levels—from frontline officers to leadership—will ensure a shared understanding of risk indicators, procedural fairness, and community engagement strategies. Integrating prevention competencies into recruitment and training is crucial for fostering a prevention-oriented culture. By embedding performance indicators and training requirements within accountability frameworks, police agencies can value prevention outcomes alongside enforcement metrics, leading to a more proactive and effective approach to community safety.



6. Policy Recommendations

Prevention is increasingly recognised as a strategic priority within European security governance and, more broadly, in contemporary risk-oriented societies. However, formal recognition alone is insufficient. It must be matched by consistent implementation, institutional integration, and the ability to demonstrate measurable impact.

To effectively prevent crime, radicalisation, and violence, policing systems require structured monitoring mechanisms. Evidence-based policing research confirms that systematic assessment tools are critical for sustainable prevention (Sherman, 2013; Hinkle et al., 2020). Regular evaluation—preferably on a quarterly basis—should include indicators such as levels of cooperation with community partners; community trust measured through procedural fairness surveys (Jackson et al., 2012); repeat incident trends in crime-concentrated locations (Weisburd, 2015); safeguarding referrals; de-escalation outcomes (Engel et al., 2020); and digital engagement metrics aligned with contemporary security strategies (European Commission, 2020). Prevention must be measurable to avoid remaining rhetorical.

Prevention before repression is not a call for softer policing, but for smarter sequencing of interventions. While the precise balance between preventive and enforcement measures may vary across Member States depending on societal conditions and legal mandates, all democratic policing systems should ensure that prevention is structurally embedded, strategically measured, and institutionally valued.

To make prevention a core function of modern policing, the following measures are recommended:

- Institutionalise prevention within strategic planning and performance frameworks, ensuring it is recognised as an essential and measurable component of policing.
- Integrate preventive objectives into existing resource allocation



and staffing models to reflect prevention in operational planning without always requiring new funding streams.

- Establish clearly designated prevention roles at the station level, with defined territorial accountability and reporting structures.
- Align community policing and intelligence-led policing through governance coordination, maintaining conceptual clarity while ensuring functional complementarity.
- Formalise multi-agency referral and safeguarding pathways, particularly for youth and vulnerable individuals, including cooperation with schools, social services, probation, and prison authorities.
- Enhance digital prevention capacity, incorporating early-warning monitoring in online environments while maintaining separation from investigative cybercrime functions.
- Embed prevention competencies in training and professional development, including communication, de-escalation, safeguarding, analytical reasoning, and digital literacy.
- Ensure preventive work is formally recognised within performance systems, including indicators that capture prevented escalation, stabilisation trends, and community trust outcomes.
- Integrate prisons and reintegration processes into the prevention ecosystem to ensure continuity between custodial and community-based interventions.
- Engage civil society in the design and evaluation of prevention strategies to strengthen objectivity, legitimacy, and alignment with shared community needs.

Strategically, the challenge is no longer to justify prevention as a priority - it is already acknowledged as such. The real task lies in strengthening implementation capacity and demonstrating its operational value through



structured metrics and visible outcomes. Only by embedding prevention within governance, resource planning, professional education, and evaluation systems can policing institutions move from declarative commitment to sustainable practice.

7. Conclusion

Sustainable public safety cannot be achieved through enforcement alone. Extensive research in procedural justice, intelligence-led policing, and radicalisation consistently demonstrates that legitimacy, trust, and early intervention are critical determinants of long-term security outcomes. Policing systems that intervene only after criminal thresholds are crossed operate at the most disruptive and costly stage of risk development. While reactive enforcement remains indispensable, disproportionate reliance on coercive measures may unintentionally deepen grievances, weaken cooperation, and reduce the flow of early-warning information essential for prevention.

Prevention-led policing should therefore not be misunderstood as a normative aspiration or a softer alternative to enforcement. It represents a strategic, evidence-based recalibration of contemporary policing. By institutionalising structured police–community partnerships, integrating analytical capacity with frontline engagement, and embedding proportionate early intervention mechanisms, police organisations can enhance operational effectiveness while reinforcing democratic legitimacy.

The central issue is no longer whether prevention matters. It is whether policing systems are structurally designed to prioritise it, measure it, and allocate resources accordingly. Aligning prevention with governance, performance frameworks, professional education, and resource planning is essential to moving from declarative commitment to operational reality.

Emphasising prevention before repression is not only consistent with European security governance; it reflects a fiscally responsible, strategically sound, and socially stabilising approach to public safety in risk-oriented



societies. The future resilience of democratic security institutions depends on their capacity to act early, proportionately, and collaboratively.

References

- Bayerl, P. S., Karlović, R., Akhgar, B., & Markarian, G. (Eds.). (2017). *Community policing: A European perspective – Strategies, best practices and guidelines*. Springer. <https://doi.org/10.1007/978-3-319-53396-4>
- Borum, R. (2011). Radicalisation into violent extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security*, 4(4), 37–62.
- Bullock, K. (2013). Community, intelligence-led policing and crime control. *Policing and Society*, 23(2), 125–144.
- Carter, J. G., & Fox, B. (2019). Community policing and intelligence-led policing: Examining the relationship between two policing models. *Policing: An International Journal*, 42(3), 446–462.
- CEPOL (European Union Agency for Law Enforcement Training). (2021). *European Union strategic training needs assessment 2022–2025*. Publications Office of the European Union. <https://www.cepola.europa.eu>
- Council of Europe HELP Programme. (2023). *Radicalisation prevention course: European standards for justice and related professionals*. Council of Europe. <https://rm.coe.int>
- Council of Europe. (2001). *European Code of Police Ethics (Rec(2001)10)*.
- Council of Europe. (2001). *European code of police ethics (Recommendation Rec(2001)10)*. Council of Europe Publishing.
- Cram, F. (2024). *Fairness, relationships and perceptions*



of police legitimacy in the context of integrated offender management. *Policing and Society*, 34(4), 250–267. <https://doi.org/10.1080/10439463.2023.2267733>

– Engel, R. S., McManus, H. D., & Isaza, G. T. (2020). Moving beyond “best practice”: Experiences in police reform and a call for evidence to reduce officer-involved shootings. *Annals of the American Academy of Political and Social Science*, 687(1), 146–165. <https://doi.org/10.1177/0002716219889328>

– European Commission. (2020). EU security union strategy 2020–2025. European Commission. <https://eur-lex.europa.eu>

– European Commission. (2023). EU Knowledge Hub on Prevention of Radicalisation. Directorate-General for Migration and Home Affairs. <https://home-affairs.ec.europa.eu>

– Fox, B. H. (2018). Community policing and intelligence-led policing: Distinct philosophies or convergent practices? *Policing: An International Journal*, 41(6), 834–849. <https://doi.org/10.1108/PIJPSM-07-2018-0105>

– Gill, C., Weisburd, D., Telep, C., Vitter, Z., & Bennett, T. (2014). Community-oriented policing to reduce crime, disorder and fear. *Campbell Systematic Reviews*.

– Hinkle, J. C., Weisburd, D., Telep, C. W., & Petersen, K. (2020). Problem-oriented policing for reducing crime and disorder: An updated systematic review and meta-analysis. *Campbell Systematic Reviews*, 16(3), e1089. <https://doi.org/10.1002/cl2.1089>

– Jackson, J., Bradford, B., Hough, M., Kuha, J., Stares, S., Widdop, S., Fitzgerald, R., Yordanova, M., & Galev, T. (2012). Trust in justice: Topline findings from the European Social Survey. European Commission.



- Kuen, K. (2024). Reassessing the process-based model: Do procedural justice and police legitimacy lead to reporting neighborhood problems to the police over time? *Journal of Criminal Justice*, 95, 102290. <https://doi.org/10.1016/j.jcrimjus.2024.102290>
- Moghaddam, F. M. (2005). The staircase to terrorism. *American Psychologist*, 60(2), 161–169.
- Pepys, R., Bowles, R., & Bouhana, N. (2020). A simulation model of the radicalisation process. *Journal of Artificial Societies and Social Simulation*, 23(4).
- Ratcliffe, J. H. (2022). *Intelligence-led policing* (2nd ed.). Routledge.
- Sherman, L. W. (2013). The rise of evidence-based policing: Targeting, testing, and tracking. *Crime and Justice*, 42(1), 377–451. <https://doi.org/10.1086/670819>
- Stephens, W., & Sieckelinck, S. (2021). Resiliences to radicalisation. *International Journal of Law, Crime and Justice*, 66.
- Sunshine, J., & Tyler, T. R. (2003). The role of procedural justice and legitimacy. *Law & Society Review*, 37(3), 513–548.
- Telep, C. W., & Weisburd, D. (2019). Is problem-oriented policing effective? *Criminology & Public Policy*, 18(2), 269–289.
- Tyler, T. R. (2006). *Why People Obey the Law*.
- Weisburd, D. (2015). The law of crime concentration and the criminology of place. *Criminology*, 53(2), 133–157. <https://doi.org/10.1111/1745-9125.12070>



Co-funded by
the European Union

THE ROLE OF SOCIAL MEDIA FOR EXTREMIST ORGANISATIONS

Holger Nitsch



1. Introduction

Social media platforms have revolutionized communication, enabling rapid sharing of information and facilitating global connectivity. However, these platforms have also been exploited by extremist organizations to spread propaganda, recruit members, and coordinate activities. Furthermore, extremist groups use social media not only to the beforementioned topics, but also for financing and cooperation and sometimes for information manipulation, that might be hand in hand with foreign state-actors information manipulation and aims to divide democratic societies. This aims to feed the extremist organisation with more possibilities to recruit personnel and gain more assets as well as it serves the purpose of the emotional aspects of extremist organisations. The vulnerable groups can mainly be identified as people in their adolescence, starting in the age of 14, and up to 30 years. Of course, there are exceptions of people that are younger or older, but this contains the target group and is in line with the group that is most vulnerable and uses social media in all its aspects. Especially during the Covid-19 pandemic the social media channels were full of material with false or wrong information, regarding the pandemic and its effects.

This misinformation combines also conspiracy theories with extremist ideologies. E.g. Right-wing groups are adopting the conspiracy theories to gain more sympathizers and followers in the virtual environment. Also, other forms of crimes developed quickly. The dark net was one big driver, but to get to a large number of people, social media is the perfect playground for gaining attention and finding followers. Several forums like 4 chan and 8 chan were platforms used for sharing extremist content and in 8 chan also live-streaming attacks, like in Christchurch, New Zealand, but this is not limited. Nowadays misinformation, extremist content is shared on any social media. Quite common are groups on Telegram, but it might be Instagram or any other tool as well. This paper expands on the role of social media in extremism by providing a detailed literature review and case studies, analysing how extremist groups leverage social media, the mechanisms of online radicalization, and policy challenges.



2. Literature Review

The literature identifies social media as a “thriving subculture” where extremists communicate, share propaganda, and recruit new members (Meleagrou-Hitchens et al., 2017). Platforms like YouTube, Instagram, and Facebook have been exploited to glorify terrorist figures and spread violent ideologies. The ability to comment, share, and send private messages fosters a “vibrant jihadist virtual community,” facilitating rapid identification and engagement among sympathizers (Meleagrou-Hitchens et al., 2017).

2.1. Social Media as a Tool for Extremist Propaganda and Recruitment

Extremist organizations worldwide use social media to disseminate their ideologies and recruit followers. Violent extremist groups such as Al-Shabaab, Boko Haram, and ISIS actively use social media to share messages, videos, and propaganda to reach global audiences (UNDP, 2022). Extremist groups have increasingly employed sophisticated online marketing techniques and IT expertise to craft and disseminate high-quality propaganda materials. According to Zeiger and Gyte (2023), terrorist organizations actively seek out skilled online marketers and IT experts to lead their propaganda campaigns, which are primarily spread via social networking sites such as Facebook, Twitter, and YouTube (p. 359). Despite efforts by platforms to remove violent extremist content, these groups remain adept at evading detection by avoiding overtly violent images or videos that trigger censorship, instead focusing on personal narratives and storytelling that resonate emotionally with potential recruits (Zeiger & Gyte, 2023).

For instance, an analysis of 1,000 pro-ISIS Facebook profiles across 96 countries in 2018 showed that ISIS’s Facebook networks continued to grow globally despite account takedown efforts (Zeiger & Gyte, 2023). These platforms are not only used for broadcasting propaganda but also for sharing personal experiences of fighters, which promotes viral imitation and emotional engagement, a potent recruitment tool.



2.2 Recruitment Strategies and Targeting Vulnerable Individuals

Extremist recruiters use social media to identify and connect with individuals who may be susceptible to radicalization. Social media's interactive features enable recruiters to engage with potential recruits by planting seeds of dissatisfaction, offering alternative identities, and providing a sense of belonging that individuals might lack offline (Zeiger & Gyte, 2023). However, to avoid police monitoring, recruiters often move conversations to encrypted messaging apps like Telegram once initial contact is made (Zeiger & Gyte, 2023).

Research in Indonesia highlights how terrorist groups such as ISIS, HTI, and JAD use social media to target youth, who are particularly vulnerable due to their ongoing identity formation and search for purpose (Jain & Vaidya, 2021). These groups exploit social media algorithms that amplify attention-grabbing content, repeatedly exposing users to extremist viewpoints and facilitating a process of self-radicalization (Jain & Vaidya, 2021). The emotional and provocative language used by extremists—words like “struggle,” “sacrifice,” and “victory”—evokes a sense of heroism and urgency, pushing individuals toward extremist action (Anas, 2020).

2.3. The Digital Transformation of Extremist Recruitment - From Physical Networks to Digital Ecosystems

Historically, extremist recruitment relied heavily on physical proximity, social networks, and direct contact. The rise of social media has dismantled these geographic and social barriers, enabling extremist groups to reach global audiences instantaneously. According to the United Nations Interregional Crime and Justice Research Institute (UNICRI), terrorist and violent extremist groups have leveraged the COVID-19 pandemic to expand their online recruitment efforts, capitalizing on increased digital engagement during lockdowns and social isolation (UNICRI, 2023).



Social media platforms like Facebook, Twitter, YouTube, Telegram, and gaming-related platforms have become primary venues for recruitment, allowing extremists to disseminate propaganda, engage in conversations, and build virtual communities (Australian Government, 2025). The shift from traditional recruitment to digital ecosystems has accelerated the radicalization timeline, reducing the time from initial exposure to active participation in extremist activities (Vision of Humanity, 2025). Important to realize is that in the past physical contact was in most cases of radicalisation crucial from a certain point on. Now this has changes as the face to face contact is due to the new technical development not necessary anymore.



3. Targeting Vulnerable Individuals: Psychological and Social Dimensions

3.1 Characteristics of Vulnerable Individuals

Extremist recruiters focus on individuals exhibiting vulnerabilities such as social isolation, economic hardship, identity crises, political disenfranchisement, and psychological distress. These vulnerabilities create fertile ground for extremist narratives promising belonging, purpose, and empowerment (Vision of Humanity, 2025).

Youth are particularly susceptible due to their developmental stage, which involves identity exploration and a heightened need for social acceptance. The European Commission emphasizes that young people facing alienation or marginalization are prime targets for radicalization via social media (European Commission, 2023).

Nevertheless, there are always exceptions to the above. Crucial analysing the studies is that there is a certain grievance mainly connected to a strong feeling of injustice. This is usually the entry int for extremist ideologies.

3.2 Psychological Manipulation Techniques

Extremist groups employ sophisticated psychological tactics to manipulate vulnerable individuals.

These include:

- Narrative Framing: Presenting extremist ideology as a solution to personal and societal grievances;
- Emotional Appeals: Using provocative language to evoke feelings of injustice, anger, and urgency (Anas, 2020);
- Social Validation: Creating online communities that reinforce extremist beliefs and provide social support (Jain & Vaidya, 2021);



- Incremental Indoctrination: Gradually exposing individuals to more extreme content to desensitize and deepen commitment (Vision of Humanity, 2025).

These tactics are often personalized, with recruiters tailoring messages based on the individual's background, interests, and online behaviour (Zeiger & Gyte, 2023).

These techniques can be used in a different framework to radicalise individuals. There is often a combination used by extremists to change the thinking and the personality of the individual recruit. One of the possibilities is mental programming. This is based on the psychological concept of mental programming, which is meant to change, individuals opinion thoughts and beliefs. This principle is found by Hofstede's cultural research, but can be misused by extremist organisations. Three phases are necessary.

In the first one there will be de-freezing, meaning the person will be mentally confused by different means like sleep deprivation, drug abuse, inundation with sensory impression and using fear and anxiety. The in the next step the mindset of the individual will be change by repetition, generating feelings of hate, monotony or creating a new language. The last step is freezing it again to have the new way of thinking long-lasting. The advantage of this methodology is that it is timely flexible and can be adjusted to the individual needs (Mansour 2022; Psychologie heute 2010).



4. Recruitment Strategies on Social Media Platforms

4.1 Content Creation and Dissemination

Extremist organizations invest in high-quality, emotionally engaging content designed to attract and retain the attention of potential recruits. This includes videos, memes, personal testimonials, and interactive posts that emphasize themes of struggle, heroism, and victimhood (Zeiger & Gyte, 2023).

The use of personal storytelling and “viral imitation” encourages users to identify with fighters and martyrs, fostering emotional connections that facilitate recruitment (Zeiger & Gyte, 2023).

4.2 Exploiting Platform Features and Algorithms

Recruiters exploit platform algorithms that prioritize engaging content, often leading to echo chambers where users are repeatedly exposed to similar extremist narratives (Prisgunanto et al., 2023). This algorithmic reinforcement accelerates radicalization by normalizing extremist views within the user’s social media feed.

Platforms’ interactive features—comments, direct messaging, group chats—enable recruiters to initiate personalized engagement, build trust, and move conversations to encrypted messaging apps like Telegram for deeper indoctrination (Zeiger & Gyte, 2023).

4.3 Use of Emerging Technologies: AI and Virtual Reality

Artificial intelligence has become a game-changer in extremist recruitment. Groups like the Islamic State Khorasan Province (ISKP) use AI to automate and personalize recruitment efforts, employing chatbots that mimic human interaction and tailor radicalization pathways based on user behavior (GNET Research, 2025).

Virtual reality (VR) is emerging as a tool for immersive indoctrination and training, allowing recruits to experience simulated combat and tactical scenarios, thereby deepening psychological commitment (Vision of Humanity, 2025).



5. Recruitment in Specific Digital Environments

5.1 Social Media Platforms

Mainstream platforms such as Facebook, YouTube, and Twitter remain central to recruitment despite content moderation efforts. Extremists adapt by using coded language, memes, and indirect messaging to evade detection (European Commission, 2023). This now can be enlarged by Instagram, Snapchat and gaming platform and is highly supported by Telegram and TikTok.

5.2 Encrypted Messaging Apps

Apps like Telegram and Signal provide secure environments for private communication, enabling recruiters to engage in direct, unmonitored conversations with potential recruits. These platforms facilitate the transition from public propaganda consumption to private indoctrination and operational planning (Zeiger & Gyte, 2023).

5.3 Online Gaming and Gaming-Adjacent Platforms

Online gaming platforms and related social spaces have become unexpected recruitment venues. Violent extremists exploit in-game chat rooms and streaming services to identify and radicalize young gamers, leveraging the interactive and immersive nature of gaming to normalize extremist narratives (Australian Government, 2025).

5.4. Fragmentation and Hybridization of Extremist Ideologies

The extremist landscape is increasingly fragmented and hybridized, with young radicals influenced by a mix of ideologies, conspiracy theories, and hybrid movements that blend far-right nationalism, religious extremism, anti-government sentiments, and anti-globalist conspiracies (Vision of Humanity, 2025). This ideological fluidity complicates recruitment monitoring and intervention.



6. Case Study

In the following there is a short description of use cases according to the virtual activities.

Case Study 1: ISKP's AI-Driven Recruitment Strategy

The Islamic State Khorasan Province (ISKP) exemplifies the integration of AI into extremist recruitment. ISKP uses AI to produce multilingual propaganda, optimize content visibility through keyword and hashtag strategies, and profile users for targeted messaging (GNET Research, 2025).

This AI-enhanced approach enables ISKP to circumvent counter-terrorism monitoring, maintain ideological cohesion, and expand its recruitment base despite territorial losses. The group's use of AI-driven chatbots for continuous engagement represents a new frontier in automated recruitment (GNET Research, 2025).

Case Study 2: ISIS and Social Media Propaganda

ISIS has been one of the most prolific users of social media for extremist purposes. The group used platforms like Twitter, Facebook, and Telegram to disseminate high-quality propaganda videos, recruit foreign fighters, and coordinate attacks globally (NIJ, 2020). Their online presence created a “virtual caliphate,” attracting thousands of recruits worldwide. Despite platform takedowns, ISIS adapted by migrating to encrypted messaging apps, illustrating the challenge of content removal.

Case Study 3: Far-Right Extremism in the United States

Data from the PIRUS dataset (2011-2016) shows that 73.2% of U.S. extremists used social media in their radicalization process, with 16.9% relying primarily on social media (START, 2018). Social media facilitated communication, sharing of propaganda, and mobilization. Notably, far-



right extremists used Facebook extensively, often supplementing offline networks. The Charleston church shooter and the New Zealand mosque attacker both used social media to livestream or publicize their attacks (Council on Foreign Relations, 2019).

Case Study 4: Al-Shabaab's Use of Social Media in Africa

Al-Shabaab uses social media to spread propaganda, recruit fighters, and intimidate local populations in East Africa (UNDP, 2022). The group exploits Facebook and Twitter to share videos glorifying attacks and to disseminate ideological narratives. Social media helps Al-Shabaab maintain influence despite military pressure, showing how online platforms sustain extremist groups in conflict zones.

Case Study 5: Right-Wing Extremist Radicalization in Europe

Research in the Netherlands and Germany reveals that social media platforms have been used to spread polarizing content that borders on extremist rhetoric (WODC, 2021). Although explicit extremist content has been reduced by platform moderation, borderline content continues to polarize users and contribute to radicalization. Recommendation algorithms sometimes amplify divisive content, facilitating “echo chambers” that reinforce extremist views.

Right-wing extremism in Europe represents a complex and evolving threat that has increasingly leveraged social media and online platforms to spread ideology, recruit followers, and coordinate activities. This phenomenon is characterized by a heterogeneous landscape of groups and ideologies, ranging from white supremacists and neo-Nazis to identitarian movements and anti-government militias, often interconnected across national borders (European Commission, 2021)2.



7. Online Ecosystem and Communication Strategies

Right-wing extremists in Europe have adapted to the digital age by exploiting a wide range of online outlets, including mainstream social media platforms such as Facebook, Twitter, and YouTube, as well as fringe and encrypted spaces like Gab, Telegram, 4chan, and BitChute (European Commission, 2021)². These platforms serve as “safe havens” for extremist content, allowing groups to disseminate propaganda, share violent manifestos, and coordinate attacks with relative anonymity and minimal oversight.

The internet has also enabled innovative operational strategies, including sophisticated financing through cryptocurrencies and crowdfunding, as well as virtual harassment tactics like doxing and trolling targeting opponents or minority groups (European Commission, 2021)². Some groups, such as the Atomwaffen Division and its European offshoots, have been formed and organized almost exclusively online, illustrating a shift toward predominantly digital extremist networks (European Commission, 2021).

8. Mechanisms of Online Radicalization

Radicalization is not simply about exposure to extremist content but involves complex social and psychological processes. Research emphasizes that radicalization requires reinforcement and social interaction, often facilitated by social media (Science Advances, 2023). Vulnerable individuals—experiencing isolation, anxiety, or rejection—are targeted through tailored messaging that offers belonging and purpose (ACT Early, 2021).

Algorithms on social media platforms can contribute to “echo chambers” or “cyberbalkanisation,” where users are exposed predominantly to like-minded views, reinforcing extremist beliefs (Meleagrou-Hitchens et al., 2017). However, some studies caution that algorithms rarely recommend extremist content directly, but radicalized users can still access and share such material (Science Advances, 2023).



8.1. Gender-Specific Recruitment and Messaging

Extremist groups also use social media to target specific demographics, including women and children. Research on Islamic State recruitment highlights gender-specific propaganda designed to appeal to women's values and social roles, using social media campaigns to groom and persuade them (NIJ, 2020). This targeted approach exploits individual propensities and social contexts, facilitated by online interactions. There is also a research project in Germany concentrating on education standard in Salafi families and is analysing education guides and online sources (not published yet).

8.2. Social Media and Far-Right Extremism

Far-right extremist groups in the United States and Europe have increasingly used social media to radicalize, mobilize, and coordinate activities. Analysis of online forums shows diverse ideological perspectives within the far-right community, with social media playing a key role in communication and planning (NIJ, 2020). Platforms have also been used to livestream attacks and spread hate speech, contributing to real-world violence (Council on Foreign Relations, 2019).

8.3. Social Media's Impact on Violence and Polarization

There is a documented correlation between hate speech on social media and spikes in violence. For example, anti-refugee attacks in Germany and communal violence in India and Sri Lanka have been linked to online hate campaigns (Council on Foreign Relations, 2019). Extremist perpetrators often self-radicalize online and use social media to publicize violent acts, amplifying their impact (Council on Foreign Relations, 2019).

8.4. Ethical and Professional Challenges

Professionals working to counter extremism face ethical dilemmas due to the public and often unregulated nature of social media. Psychologists and



social workers must navigate privacy concerns while engaging in online counter-radicalization efforts (American Psychological Association, 2021).

Mainstreaming and Normalization Tactics

A key strategy employed by right-wing extremists in Europe is the normalization of their ideologies through “metapolitical” approaches aimed at shifting public discourse and expanding the boundaries of acceptable political debate (European Commission, 2021)². Movements like the Identitarians focus less on electoral politics or violent street action and more on influencing the “dominant zeitgeist” by injecting terms such as “remigration” and “genderismus” into public conversations.

These groups often use humour, sarcasm, memes, and conspiracy theories to package extremist views as “just jokes,” thereby making them more palatable to a broader audience and shielding themselves from criticism (European Commission, 2021)². This strategic use of online culture facilitates the spread of fake news and the undermining of expertise, contributing to a polarized and fragmented information environment.

Transnational Networks and Offline Links

Right-wing extremist movements in Europe are not confined by national borders. The conflict in eastern Ukraine, for example, has become a hub for foreign fighters and a physical nexus for right-wing extremist networks (European Commission, 2021)². Moreover, extremists participate in international rallies, concerts, and events to forge personal and organizational ties, reinforcing a transnational extremist subculture.

Impact of Social Media on Political Populism and Extremism

Recent studies indicate that social media significantly influences the rise of populist and extremist political movements across Europe. Research published in ScienceDirect (2024) demonstrates how social media platforms have been instrumental in amplifying far-right populist votes and



spreading extremist narratives, contributing to political polarization and the erosion of democratic norms (ScienceDirect, 2024)¹.

Recent Trends and Challenges

The COVID-19 pandemic and related conspiracy theories, such as those surrounding 5G technology, have been appropriated by right-wing extremists to expand their reach and recruit new followers (European Commission, 2021)². Movements like the “yellow vests” protests in some countries have been infiltrated by extremists, blurring the lines between legitimate dissent and extremist mobilization.

The European Union and member states have recognized the increasing threat posed by right-wing extremism. Europol’s 2020 Terrorism Situation and Trend Report highlights the growing use of the internet by right-wing extremists to livestream attacks, disseminate manifestos, and radicalize individuals globally (European Commission, 2021)². The transnational nature of these groups necessitates coordinated intelligence sharing and joint counter-terrorism efforts.



9. Challenges and Policy Implications

The risks for security and safety are obvious and the key question is what is necessary to mitigate the risks evolving from radicalisation and the fast technological development in social media and the misuse of these. The technological innovation is developing in an enormous speed and countering the unfortunately innovative misuse by extremist organisations is crucial. Reflecting the above this results in several challenges and policy implications.

9.1 Challenges

In short there are several key challenges to mitigate the risk and counter the threat emerging:

Platform Moderation Limitations: Extremists' use of coded language and migration to encrypted platforms limits the effectiveness of content removal (Zeiger & Gyte, 2023).

Algorithmic Amplification: Social media algorithms inadvertently promote extremist content by prioritizing engagement (Prisgunanto et al., 2023).

Youth-Generated Extremist Content: Increasingly, youth themselves produce and share extremist material, complicating the traditional victim-perpetrator dynamic (Australian Government, 2025).

Technological Sophistication: AI and VR technologies enhance recruitment sophistication, outpacing current countermeasures (GNET Research, 2025).

9.2 Policy Recommendations

Countering violent extremism and radicalisation with respect of the influence of social media in this process is essential to create a safe and se-



cure society. Several policy recommendations result from the challenges and the above described methodologies, risks and threats:

- Enhance Digital Literacy: Equip youth with critical thinking skills to recognize and resist extremist narratives (Etumnu & Williams-Etumnu, 2023);
- Strengthen Platform Accountability: Mandate transparency in content moderation and cooperation with law enforcement (European Commission, 2023);
- Develop AI-Based Countermeasures: Invest in AI tools for detecting and countering extremist propaganda (GNET Research, 2025);
- Foster Multi-Stakeholder Partnerships: Governments, tech companies, educators, and civil society must collaborate to address recruitment challenges (Australian Government, 2025);
- Support Community Resilience: Build social support networks to reduce vulnerabilities exploited by extremists (Vision of Humanity, 2025).



10. Conclusion

Social media plays a critical role in the operations of extremist organizations, enabling propaganda dissemination, recruitment, radicalization, and coordination of violence. The literature and case studies demonstrate the complexity of online radicalization and the challenges in balancing security with rights to free expression. Effective policy responses require multi-faceted approaches involving technology regulation, community-based interventions, and international cooperation.

Social media's role in facilitating extremist organizations, particularly right-wing extremists in Europe, is multifaceted and deeply consequential. The digital environment has become a critical battleground where extremist ideologies are propagated, normalized, and operationalized. Right-wing extremists exploit social media's reach and anonymity to spread hateful narratives, recruit vulnerable individuals, and coordinate violent acts, often transcending national borders and leveraging both online and offline networks.

The literature and case studies reviewed underscore that social media platforms do not act in isolation to cause radicalization but serve as powerful enablers and accelerators of extremist processes. Algorithms and platform designs can inadvertently amplify polarizing content, while extremist groups skilfully use memes, humour, and coded language to mainstream their ideas and evade moderation.

Policy responses must therefore be comprehensive and adaptive, balancing the imperative to protect democratic societies from extremist violence with the need to uphold freedom of expression and privacy. This includes enhancing platform accountability, regulating algorithmic amplification, investing in digital literacy, and fostering international cooperation. Moreover, addressing the socio-economic and psychological vulnerabilities that extremists exploit remains essential.

The rise of right-wing extremism in Europe, as evidenced by recent vio-



lent incidents, online mobilization, and the mainstreaming of extremist discourse, demands urgent and sustained attention from policymakers, civil society, and technology companies alike. Only through coordinated, multi-dimensional strategies can the complex challenges posed by extremist use of social media be effectively mitigated, preserving social cohesion and democratic resilience.

Furthermore, IT professionals should educate social scientists about using online tools to analyse Internet content (Scrivens et al. 1, 2020: pp. 1417-1435). Also, some sociologists and criminologies point out that radicalisation in the social sciences cannot be reduced exclusively to a security approach, but it is necessary to analyse the motivation of extremist actors, opportunities and expand this discussion to the level where radicalisation becomes a cognitive problem of society. The Internet helps to understand new forms of adopting some values and norms of another culture. Social networks (e.g. Twitter, Facebook) are also used to break ties with familiar people and establish connections with strangers (Khosrokhaver, 2014).



11. References:

Note: The research was supported by Perplexity AI

- Act Early (2021): Radicalisation and the Internet
- American Psychological Association. (2021). Ethical challenges in social media and extremism.
- Anas, M. (2020). Emotional and Provocative Language in Extremist Propaganda. *Journal of Terrorism Studies*.
- Australian Government. (2025). Australia's Counter-Terrorism and Violent Extremism Strategy.
- Council on Foreign Relations. (2019). The role of social media in extremism.
- European Commission. (2021). Contemporary manifestations of violent right-wing extremism in the EU.
- European Commission. (2023). Prevention of radicalisation.
- GNET Research. (2025, April 11). Automated Recruitment: Artificial Intelligence, ISKP, and Extremist Radicalisation.
- Hassan, R., et al. (2022). Marketing Strategies of Extremist Groups on Social Media. *Journal of Digital Extremism*.
- International Centre for Counter-Terrorism (ICCT). (2023). Right-wing & anti-government extremism.
- Jain, S., & Vaidya, S. (2021). A Study on the Role of Social Media in Radicalization and Terrorism. *Akta*, 419-430.
- Jati, R., & Mamoto, A. (2021). Covert Communication Strategies in Online Extremism. *Cybersecurity Review*.
- Khosrokhavar, F. (2014). *Radicalisation*. Paris: MSH PARIS.
- Mansour, A (2022). Interview, *Psychologie heute* Ausgabe 3
- Meleagrou-Hitchens, A. et al. (2017). The impact of digital communications technology on radicalization and recruitment. Chatham House.
- Prigunanto, H., et al. (2023). Social Media and Self-Radicalization



Among Youth. *International Journal of Security Studies*.

- Psychologie heute Ausgabe 3/2010
- Ressa, M (n.d.). How to stand up a dictator. Goodreads.
- Saltman, E., & Smith, M. (2015). Women and Online Jihadist Propaganda. *Studies in Conflict & Terrorism*.
- ScienceDirect. (2024). Online social media and populism in Europe.
- Scrivens R., Gill P., Conway M. (2020) The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research. In: Holt T., Bossler A. (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_61
- Shaw, A. (2023). Social media, extremism and radicalization. In *Science Advances*
- United Nations Interregional Crime and Justice Research Institute (UNICRI). (2023). Malicious use of social media by terrorists, extremists, and criminals.
- United Nations fact finding Mission (2019): Hate Speech on Social Media. In *Council of Foreign Relations*.
- Vision of Humanity. (2025, March 21). Youth Radicalisation: A New Frontier in Terrorism and Security.
- Winter, C. (2015). Women in ISIS: Propaganda and Recruitment. *International Centre for the Study of Radicalisation*.
- Zeiger, S., & Gyte, D. (2023). Prevention of Radicalization on Social Media and the Internet. In *Handbook of Terrorism Prevention and Preparedness* (pp. 359-370). *International Centre for Counter-Terrorism*.



HOW DO RELIGIOUSLY EXTREMIST ACTORS USE ONLINE ENVIRONMENTS FOR RECRUITMENT - AND WHAT CONCLUSIONS CAN BE DRAWN FROM THIS FOR POLICE PREVENTION WORK?

Col. Holger Schmidt



1. Introduction, objectives, and methodology

1.1 Introduction to the topic

Today, the recruitment of young people by religious extremist actors takes place to a large extent in digitally mediated communication spaces (RAN 2022). Social networks, messenger services, and video platforms enable extremists to reach very different target groups in a short period of time, build relationships, and gradually integrate them into radical milieus (Gill et al. 2017; RAN 2022). This raises the question for practitioners in the police, security agencies, and civil society of how online recruitment actually works and where effective interventions are possible (RAN 2022).

The 225 security-related cases from 2016 to 2018 evaluated as part of a Bavarian exit program already show that social media platforms represent the entry point into Islamist extremist radicalization for a large number of those affected (Schüler 2017). In many cases, the process begins with the consumption of propagandistic preacher videos, for example by Salafist actors, whose content specifically addresses patterns of reception in youth culture (Schüler 2017). Building on this, contact is established with members of the scene via social networks, which in some cases can lead to massive changes in attitudes, conflicts in the parental home, and security-relevant behavior within a few weeks (Schüler 2017).

his is impressively illustrated by the case of 13-year-old „Marie K.“ (pseudonym), who grew up in a small Bavarian town without a family migration background. After a phase of intensive use of computers and smartphones, her mother noticed significant withdrawal and changes in attitude. The trigger for concern was ultimately a heated argument in which Marie called her mother a „kuffar slut“ – a term that her mother was only able to identify after conducting her own internet research. Research revealed that Marie had initially entered the scene via online sermons by a Salafist preacher and had then specifically contacted relevant actors via social networks.



Within about two months, she had developed a superficial but security-relevant interest in Islamist extremist content, which required rapid intervention by counseling centers and the police (Schüler 2017).

The intertwining of online communication, the world of young people, and extremism becomes even clearer in the case of 18-year-old „Tim K.“. He posted a message in a school WhatsApp group chat saying that his „lifelong dream“ was to „die in jihad“ and, at the same time, carved the logo of the so-called „Islamic State“ into school desks. The subsequent investigation revealed intensive online engagement with jihadist propaganda and online preachers, as well as contacts with individuals at so-called Koran distribution stands (Schüler 2017). The case exemplifies how online recruitment impulses—propaganda and establishing contact—can intersect with youthful rebellion, status seeking, and provocative behavior and lead to situations that require police intervention (Schüler 2017).

At the same time, case studies show that online recruitment rarely happens in isolation (Schüler 2017; RAN 2022). In almost all cases examined, personal contacts within the extremist milieu were found—often after initial digital engagement—which stabilized and deepened the process. For example, 15-year-old „Lisa-Marie A.“ initially used social media platforms to compensate for loneliness after moving to a rural area, where she made contact with Salafist actors. This led to the development of romantically coded online relationships that facilitated her entry into a Salafist lifestyle and made it difficult for her to distance herself from it for years (Schüler 2017). These and other cases underscore that while online recruitment is often the visible trigger, the lasting consolidation of radical attitudes is almost always linked to relationship building—both online and offline (RAN 2022).

Empirical syntheses by the Radicalization Awareness Network (RAN) come to similar conclusions (RAN 2022). The central RAN report „Online Radicalisation – What we know“ emphasizes that the internet should primarily be understood as a catalyst and amplifier of already established



radicalization processes, enabling propaganda, networking, recruitment, and organizational functions at high speed and range (RAN 2022). At the same time, RAN highlights the limited evidence available and the need to always consider online radicalization and recruitment in conjunction with individual vulnerabilities, social contexts, and offline relationships (RAN 2022; Gill et al. 2017).

1.2 Objectives and methodology of the article

Against this background, this article pursues two objectives.

First, it aims to identify how religious extremist actors specifically use online environments for recruitment: Which communication spaces and platforms are used, which narratives and aesthetic forms dominate, and what role do peers, „micro-influencers,“ and personal relationships play? (RAN 2022; RAN 2021).

Second, based on RAN findings and academic literature, it aims to develop practical implications for prevention and intervention that are particularly relevant for the police, security authorities, exit programs, and other first points of contact (RAN 2022; El Difraoui et al. 2021).

The article combines three strands of knowledge:

- RAN publications on online radicalization and the role of digital communication spaces in recruitment processes.
- The international state of research on online extremism, social media-based recruitment strategies, and radicalization processes in jihadist religious extremism.
- Practice-based case studies from a Bavarian exit program, which have already been published in edited form and provide concrete insights into the dynamics of online recruitment and deradicalization.



2. Terms, context, and framework

2.1 Online recruitment

In the following, online recruitment refers to the use of digital communication spaces, in particular social media, messenger services, forums, video and gaming platforms, to systematically introduce individuals to religious extremist scenes, bind them to these scenes () and, in the long term, win them over for supportive or activist actions (RAN 2022; Gill et al. 2017).

It involves more than simply „exposing“ extremist content: the decisive factors are the transition from general online propaganda to the targeted identification of vulnerable individuals, personal contact (often via direct messages or closed groups), and the establishment of stable, usually emotionally charged relationships (RAN 2022).

Case studies from Bavaria show that social media plays at least three roles: as a medium for public information and propaganda, as a stage for rebellion and status communication, and as an amplifier of emotional appeal and relationship building (Schüler 2017). In many cases, the development begins with the consumption of relevant videos (e.g., sermons by Salafist actors), continues with participation in comment columns, groups, and chats, and culminates in individually tailored contact and offers of commitment (Schüler 2017). Complete radicalization and recruitment processes without real-life contacts remain the exception; the internet is primarily an accelerator and range extender, not the sole cause (RAN 2022; Schüler 2017).

In a narrower sense, online recruitment is therefore understood as a sub-process of online radicalization: it follows on from initial exposure to extremist content, uses digital spaces to create a sense of belonging and identity, and often prepares the transition to offline networks (RAN 2022).



2.2 Religious extremism, Islamism, and Salafism

For the present analysis, it is essential to clarify terminology, as terms such as „religious extremism,“ „Islamism,“ and „Salafism“ are not used uniformly in academia, practice, and the public sphere (Pfahl-Traughber 2019; El Difraoui et al. 2021).

Following the Federal Office for the Protection of the Constitution, extremism is defined as an effort to eliminate the fundamental values of the free democratic basic order (BfV 2017). In addition, social science literature emphasizes that extremist ideologies are typically characterized by a worldview that is understood as superior, an absolute claim to truth, rigid friend-foe schemata, and the subordination of the individual to a supposedly higher collective interest (Neumann 2016; Abou-Taam 2014).

Islamism can be understood in Pfahl-Traughber's sense as a collective term for political views and actions that seek to establish a social and political order legitimized solely by religion in the name of Islam (Pfahl-Traughber 2019).

The goal is a theocratic order in which Islam is not only an individual way of life, but also a binding guideline for the state and society (Roy 2003). The use of violence is not a mandatory feature; Islamist actors can act in a legalistic, missionary, or charitable manner, while violence-oriented movements can be classified as jihadist terrorism (Neumann 2016; Doosje et al. 2016).

Salafism, on the other hand, represents a specific variant of Sunni Islamism that is particularly relevant in Germany (Bauknecht 2018; Abou-Taam 2014). Salafist actors propagate a return to a supposedly „original“ form of Islam, reject Western concepts of democracy and human rights, and proclaim that they represent „true Islam“ (BfV 2012; Neumann 2016). In Germany, the Salafist scene has developed within a few years from a small network of preachers into a movement shaped by youth culture, which is particularly appealing to teenagers and young adults due to its



media-savvy communication, simple answers, and strong group identity (Abou-Taam et al. 2016; El Difraoui et al. 2021).

Religious extremism in the narrower sense is understood here as an umbrella category within which jihadist Islamism and, in particular, violent Salafism play a central role (Doosje et al. 2016). This article therefore focuses on online recruitment processes within this spectrum, without ignoring other forms of religiously motivated extremism.

2.3 Radicalization and the online dimension

Following on from Schmidt and Schüler, radicalization can be described as a process in which individuals gradually become more receptive to extreme ideologies and, in some cases, develop a willingness to accept violence as a legitimate means of achieving political and religious goals (Schüler 2017). There is no such thing as „the“ typical path to radicalization or a uniform set of standard factors; rather, models such as those developed by Moghaddam, Silber/Bhatt, Precht, Sageman, and Borum show a variety of possible trajectories and influencing factors (Moghaddam 2005; Silber/Bhatt 2007; Sageman 2004; Borum 2011). It is crucial to understand radicalization as a dynamic, context-dependent process with individual, social, political, and ideological dimensions (Doosje et al. 2016).

In his qualitative study of the radicalization processes of Islamists, Schüler identifies key areas of influence, including religion/ideology, sense of community, reference persons, political perceptions, propensity to violence, personal prerequisites, and specific contexts such as prison, the internet, and targeted recruitment (Schüler 2017).

Particularly relevant to online recruitment are the findings on community spirit and initial contacts with the scene: many respondents were experiencing identity or life crises before turning to the Salafist milieu, seeking orientation, belonging, and clear rules, and found these in the dichotomous worldview of Salafism (Schüler 2017; Pfundmair/Schmidt



2019). The internet often served as an entry channel and a space for initial contact with like-minded people (Schüler 2017).

In Schüler's work, as well as in Schmidt's anthology contribution, the online dimension is described as an important but not solely decisive factor (Schüler 2017; Schmidt 2018). The internet and social media contribute to the removal of geographical boundaries, identity-forming networking, and the emotional staging of conflicts; at the same time, the evaluation of case files and interviews shows that purely virtual radicalization processes are rare and that personal contacts play a central role in consolidation (Schüler 2017). This assessment is consistent with RAN findings, according to which the internet primarily acts as a catalyst that facilitates propaganda, community experience, and recruitment without replacing offline relationships (RAN 2022).

2.4 RAN as an analytical and practical framework

From 2011 to 2024, the European Union's Radicalization Awareness Network (RAN) provided the overarching framework for this analysis (RAN 2022). During this period, RAN brought together practitioners from the police, judiciary, social work, education, research, and civil society across Europe with the aim of pooling knowledge on radicalization, prevention, and deradicalization and making it accessible in the form of papers, handouts, and collections of practices (RAN 2021). The Radicalisation Awareness Network (RAN) was gradually replaced by the EU Knowledge Hub on Prevention of Radicalisation as the new central EU structure in the course of 2024 (Start Insight 2024).

With regard to online recruitment, two RAN strands are particularly relevant:

The thematic report „Online Radicalisation – What we know,“ which synthesises empirical findings on the role of the internet in the radicalisation process and distinguishes between functions such as propaganda,



networking, recruitment, and operationalisation. Among other things, it emphasizes the limited quality of evidence, the hybrid nature of online and offline, and the need to situate online phenomena in broader social contexts (RAN 2022).

The work of the Working Group Communication & Narratives (RAN C&N), which deals with extremist narratives, online communication, social media strategies, and counter and alternative narratives, and provides a practical planning and evaluation grid for communication campaigns with the GAMMMA+ model (RAN 2021).

RAN does not view online recruitment as an isolated technical process, but rather as a communicative and relationally embedded practice of extremist actors (RAN 2022). The conceptual definitions used here—for online recruitment, religious extremism, Islamism/Salafism, and radicalization—are therefore based on RAN concepts, but are concretized by Schmidt’s empirical case analyses and Schüler’s qualitative results (Schüler 2017; Schmidt 2018). This is to ensure that the rest of the article is both compatible with the European discourse and remains directly anchored in German prevention and deradicalization practice.



3. State of research on online radicalization and recruitment

3.1 Online radicalization: overview

Early work on terrorism on the internet described the web as a multipurpose tool for psychological warfare, propaganda, data collection, fundraising, recruitment, mobilization, networking, and operational coordination (Conway 2006; Sageman 2004). As early as 2004, Sageman warned of the possibility that online communities could create close bonds between individuals and virtual scenes—facilitated by instant feedback, the absence of moderating countervoices, and seemingly simple ideological solutions (Sageman 2004).

Current syntheses—such as the RAN report „Online Radicalization—What We Know“—paint a much more nuanced picture (RAN 2022). Violent groups systematically use the internet to disseminate information, build networks, recruit, finance, and gather information (RAN 2022; Gill et al. 2017). At the same time, the evaluation of case studies shows that the role of the internet depends heavily on the individual case : in some biographies, the online dimension is central, in others it is more complementary, and in still others it is hardly relevant (RAN 2022).

Whittaker and others therefore typically classify the functions of the internet in the radicalization process into several categories: information provision (propaganda), community building and identity formation, recruitment and mobilization, logistical support, and information gathering (Whittaker 2022).

It is important to note that online radicalization is usually not a linear, solely digital process, but remains closely intertwined with offline experiences of marginalization, personal crises, group affiliation, and physical contacts (RAN 2022; Gill et al. 2017).



3.2 Social media and radicalization: findings from reviews

Several systematic reviews examine how social media influences radicalization processes. Akram and Nasar synthesize 82 peer-reviewed studies on „radicalization through social media“ and identify two central topics: determinants of radicalization on social media platforms and measures to contain and deradicalize content (Akram/Nasar 2020). Their analysis shows, among other things, that political interests, loss of trust in state institutions, and actively searching for radical content are important drivers, while mere exposure alone is typically not enough (Akram/Nasar 2020).

The review also emphasizes that social media primarily promotes three effects: first, the dissemination of propaganda and conspiracy narratives with a wide reach; second, the formation of echo chambers and homophilic networks; and third, easier contact between like-minded individuals and potential recruiters (Akram/Nasar 2020). At the same time, the authors identify significant gaps in research: the effects vary depending on the regional context and target population, and experimental or intervention-oriented studies are rare to date (Akram/Nasar 2020).

Another overview on „Online extremism: Research trends in internet activism, radicalization, and countermeasures“ shows that violence-oriented organizations use online tools primarily for propaganda, recruitment, logistics, financing, and hacking, while individuals use the internet primarily for socialization, learning, and identity formation (Conway et al. 2019). Existing research confirms that the internet can facilitate radicalization, but at the same time points out that clear causal relationships—in the sense of „the internet causes radicalization“—are difficult to prove empirically (RAN 2022; Conway et al. 2019).

3.3 Online recruitment in religious extremism

With regard to religious extremists, especially jihadists, online recruitment can be described as one of several core functions of Internet use (Gill et al. 2017; RAN 2022). Both the RAN Online Report and various



empirical studies show that organizations such as the so-called „Islamic State“ made intensive use of social media platforms to generate international reach and target sympathizers (RAN 2022; Conway et al. 2019).

According to estimates, there were at times tens of thousands of IS-supporting Twitter accounts, and fighters who had left their countries „streamed“ their lives in conflict zones to their countries of origin in near real time (Berger/Morgan 2015; RAN 2022).

Case studies and individual case analyses illustrate typical recruitment channels: First, broad, often aesthetically appealing propaganda is disseminated via open platforms (e.g., YouTube, Instagram, TikTok), appealing to emotions such as outrage, pride, belonging, and a thirst for adventure (Gill et al. 2017). Interested or vulnerable individuals are identified through likes, comments, and shared content and then transferred to semi-public or closed communication channels (e.g., Facebook groups, Telegram channels, private chats) (RAN 2022). There, recruiters and members of the scene intensify the relationship, respond to personal crises, answer religious and political questions, and convey a sense of exclusive community (Gill et al. 2017; RAN 2022).

The Bavarian case studies underscore this process logic: in the vast majority of the 225 cases examined, social media platforms initially served as a medium for propaganda and contact before personal contacts were established in the real world (Schüler 2017). In the case of „Marie K.,“ for example, sermon videos by a Salafist preacher, combined with social media contacts, led to a clearly perceptible ideological shift and severe family conflicts within two months, without there already being any established involvement in physical networks (Schüler 2017). Other cases, such as „Armin O.,“ show that online recruitment can also lead to profound ideological radicalization in individuals without direct access to local scenes—in his case, to the point of actively supporting jihadist fighters by creating and maintaining social media accounts (Schüler 2017).



Schüler's qualitative interviews with dropouts and experts confirm that the internet and social media often provide the initial contact with the Salafist scene and play an important role in recruitment (Schüler 2017). However, his evaluations show that fully developed radicalization processes are almost always stabilized by personal references, local groups, or charismatic leaders (Schüler 2017). Online recruitment thus appears to be a „door opener“ and accelerator—the decisive factor remains whether and how these contacts are transferred into real networks of relationships (Schüler 2017; RAN 2022).

3.4 Evidence, limitations, and controversies

Both RAN and scientific reviews emphasize that, despite a growing body of literature, the evidence on online radicalization and recruitment remains limited and heterogeneous (RAN 2022; Akram/Nasar 2020). Many studies are based on publicly available online data, case studies, or expert assessments; systematic longitudinal or intervention studies are rare (Conway et al. 2019). Methodological challenges arise from data protection, ethical issues, access restrictions to closed groups, and the difficulty of clearly assigning online interactions to individual persons or biographical histories (RAN 2022; Gill et al. 2017).

RAN explicitly points out that the role of the internet as a „driver“ of radicalization has often been and continues to be overestimated (RAN 2022). The report emphasizes that online factors must always be viewed in conjunction with individual vulnerabilities (e.g., identity crises, psychological stress), social contexts (family, peers, school, community), and political conditions (experiences of discrimination, conflicts) (RAN 2022; Doosje et al. 2016). Individual perpetrators who are purely „radicalized online“ remain the exception; far more often, online and offline experiences overlap - a finding that is confirmed in particular by the evaluation of radicalization biographies (Schüler 2017).



The following topics are particularly controversial in the literature:

How strongly social media should be weighted as an independent risk factor compared to existing radicalization tendencies (Akram/Nasar 2020; RAN 2022). Whether certain platforms or formats (e.g., gaming environments, encrypted messengers, short video apps) actually open up qualitatively new recruitment opportunities or rather dress familiar patterns in new technical guises (Whittaker 2022; Conway et al. 2019). To what extent measures such as content takedowns, algorithmic filters, or counter-narrative campaigns can measurably influence radicalization and recruitment processes (RAN 2021; Gill et al. 2017).

For practitioners, this means that the current state of research provides a range of reliable information on the functions of the internet and typical recruitment paths, but only allows cautious statements to be made about the causality and effectiveness of individual measures (RAN 2022; Akram/Nasar 2020). This makes it all the more important to combine empirical findings with practical case studies—such as those from Schmidt's exit program—in order to gain a realistic picture that neither dramatizes nor downplays the impact of online recruitment (Schüler 2017).



4. Mechanisms and practices of online recruitment

4.1 Communication spaces and platforms

Today, the online recruitment of religious extremists takes place in an ecosystem of open, semi-public, and closed spaces (RAN 2022; Conway et al. 2019). Open platforms such as YouTube, Instagram, TikTok, and public Facebook pages serve primarily as showcases for propaganda, sermon videos, campaigns, and symbolic performances (Gill et al. 2017). Semi-public and closed communication spaces—such as messenger services, group chats, or private channels—are used to filter out those users who appear particularly receptive from the mass of users and transfer them to more intensive communication (RAN 2022).

The Bavarian case studies clearly illustrate this (Schüler 2017). „Marie K.“ became involved in Salafist-influenced content through sermon videos distributed online and then used Facebook to make contact with members of the scene who were specifically looking for young people like her (Schüler 2017). „Tim K.“ used a school WhatsApp group chat to post a jihadist coded message („My life’s dream is to die in jihad“); in addition, he conducted an intensive online search for preacher content and contacts via social media (Schüler 2017). In both cases, open and semi-public spaces served as a recruitment platform and as an environment in which initial signals could be sent and picked up (Schüler 2017).

A more recent development concerns gaming platforms and streaming-related services (Europol 2023; RAN 2022). In the case of the 18-year-old perpetrator of the attack in Munich on September 5, 2024 — who attempted to attack police officers and, presumably, the diplomatic mission near the Israeli Consulate General and the NS Documentation Center — investigators found, among other things, older computer game videos with Islamist content and symbols of the group Haiat Tahrir al-Sham (HTS) on his devices (Bayerisches LKA 2025). The young man had already used corresponding HTS symbols in a computer game at the age



of 14; seized clips showed how Islamist scenes of violence were playfully processed (Bavarian State Office of Criminal Investigation 2025). The case shows how gaming contexts can function as entry points where extremist symbols, scenes of violence, and narratives are initially taken up in a supposedly „ironic“ or experimental way and then ideologically transformed (Europol 2023).

Europol and other actors point out that gaming and streaming platforms are now being misused to a considerable extent for the dissemination of extremist content and for recruitment, especially of young people (Europol 2023; RAN 2021).

Staged reenactments of terrorist attacks in 3D gameplay, accompanied by extremist music and symbols, are recorded, edited, and then disseminated on mainstream platforms (Conway et al. 2019). This shifts part of the preliminary stages of recruitment to spaces that have long been largely ignored by prevention practitioners and security authorities (RAN 2022).

4.2 Narratives, aesthetic forms, and emotional appeals

RAN publications and empirical studies show that online recruitment relies heavily on narratives and emotional appeals (RAN 2021; RAN 2022). Typical examples include dichotomous „us versus them“ narratives, victim narratives („the global umma is being oppressed“), heroic stories of fighters, and promises of salvation and meaning (Doosje et al. 2016; Neumann 2016). This content is translated into aesthetically appealing formats: high-gloss videos, music, memes, short clips, and story formats that deliberately pick up on youth reception patterns (Conway et al. 2019).

The case studies examined show how such narratives tap into individual needs (Schüler 2017). „Marie K.“ was looking for validation and guidance; through videos of a prominent Salafist preacher, she encountered simple, absolute truths, clear rules, and an offer of belonging to a supposedly „pure“ community (Schüler 2017). „Sarah F.“—marked by loneliness,



mental instability, and a lack of family stability—used social networks to connect with people who were discussing traveling to Syria and Iraq and presented her with an idealized Salafist lifestyle, including romanticized images of partnerships and families (Pfundmair/Schmidt 2019). In her case, the need for love, protection, and belonging was combined with on-line narratives of religious chosenness and communal strength (Pfundmair/Schmidt 2019).

„Lisa-Marie A.,” who suffered from loneliness after moving to a rural area, initially used social networks to compensate for her lack of contacts (Schüler 2017). Using several accounts, some of them anonymous, she formed relationships, fell in love online with a Salafist man from abroad, and became increasingly drawn into a Salafist parallel world in which love, loyalty, and religious duty were intertwined (Schüler 2017). This shows how online recruitment specifically combines youth cultural themes (love, relationships, rebellion) with religious extremist motives (RAN 2021).

Emotional and social factors also played a central role in the Munich case of February 13, 2025, in which a 24-year-old Afghan asylum seeker drove a vehicle into a Verdi demonstration, injuring dozens of people (Bayerisches LKA 2025).

According to investigations, his radicalization began about six months before the attack, triggered in particular by growing debts, a lack of prospects, and massive integration problems (Bavarian State Office of Criminal Investigation 2025). In the absence of viable real-life contacts, he increasingly withdrew into online forums, where he encountered extremist content and Islamist ideologies; His online communications contained references to Islamist motives, but no firm organizational ties could be proven (Bavarian State Office of Criminal Investigation 2025). The case underscores how online narratives can provide meaning in situations of subjective overload and at the same time legitimize violence as a supposedly logical response (RAN 2022).



4.3 Roles of recruiters, peers, and „micro-influencers“

Online recruitment is rarely the result of anonymous mass communication; as a rule, specific actors intervene who act as recruiters, peers, or „micro-influencers“ (RAN 2021; Gill et al. 2017). In Schüler's study, which he conducted with the support of the Bavarian State Criminal Police Office, and in Schmidt's case studies, three groups repeatedly appear (Schüler 2017):

- Ideologically trained scene actors who deliberately seek out vulnerable individuals and approach them via social media, messenger services, or gaming platforms.
- Peers of the same age who share, comment on, and normalize content, thus acting as door openers into scene milieus.
- Prominent preachers or influencers whose videos and posts create a kind of „ideological background noise“ that personal contacts then build on.

In the case of „Marie K.," this structure is clearly recognizable: the initial influence of a prominent preacher, the subsequent networking with scene actors via Facebook, and the attempt to draw her into a more radical bubble (Schüler 2017). In the case of „Tim K.," the peer-communicative dimension comes to the fore: the message in the class chat was clearly aimed at provocation, status gain, and distinction—embedded in an online context in which jihadist content was already present (Schüler 2017).

Based on current findings, the perpetrator of the Munich shooting attack on September 5, 2024, appears to have been „inspired“ rather than organizationally involved (Bavarian State Office of Criminal Investigation 2025).

Although authorities found evidence of Islamist symbols and content in computer games and on his cell phone, they found no reliable evidence of direct control by a group (Bavarian State Office of Criminal Investigation 2025).



tion 2025). In the case of the vehicle attack on the Verdi demonstration in 2025, investigators currently assume that the perpetrator acted alone and that his online communications indicate Islamist-motivated radicalization, without any clear links to specific organizations being detectable (Bavarian State Office of Criminal Investigation 2025).

These constellations - loosely inspired lone perpetrators who become ideologically charged in online environments without any fixed organizational ties—pose particular challenges for prevention and law enforcement (RAN 2022). At the same time, Schmidt's exit experiences show that even in the case of supposed „lone actors,“ there are often at least temporary online relationships with radicalized individuals or groups, for example in the form of closed chat groups or supporter communities (Schüler 2017).

4.4 Process logic of online recruitment

Based on RAN material, international studies, and Schmidt's case analyses, a typical—though not necessarily linear—process logic of online recruitment can be outlined (RAN 2022; Gill et al. 2017).

Exposure

First contact with extremist content via open platforms (videos, memes, posts, gaming scenes), often during periods of personal searching, crisis, or boredom (RAN 2022). In the case of „Armin O.,“ this included online videos of a Salafist preacher, and in the case of the perpetrator of September 5, 2024, Islamist-coded gaming content (Bayerisches LKA 2025).

Resonance and identification

Certain narratives or symbols trigger resonance: a sense of justice, belonging, rebellion, strength, or spiritual meaning (Doosje et al. 2016). In the cases of „Sarah F.“ and „Lisa-Marie A.,“ loneliness and the search for love and belonging were central points of connection that were addressed



by online community and relationship offers (Pfundmair/Schmidt 2019; Schüler 2017).

Establishing contact and selection

Interested individuals are identified through likes, comments, shared content, or direct messages (Gill et al. 2017). Recruiters or peers make contact, invite people to chats, groups, or channels, and check their reactions (RAN 2022). In many of the cases studied, communication quickly shifted from open platforms to messenger services such as WhatsApp (Schüler 2017).

Intensification and support

The relationship is deepened in semi-public or closed spaces: permanent availability, answering religious/political questions, emotional support, building a sense of „togetherness“ (RAN 2022). Case analyses show that in some cases, hundreds of messages were sent per day to emotionally bind those affected (Schüler 2017).

Transfer to offline structures or more conspiratorial online networks

Where possible, face-to-face meetings are arranged (e.g., at Koran stands, in mosques, apartments), or contacts are transferred to structures that are more difficult to access (encrypted messengers, smaller cells) (Gill et al. 2017). In the case of „Anna B.,” for example, an online order for a Koran led to Salafist activists appearing at her accommodation and beginning intensive offline relationship-building work (Schüler 2017).

Mobilization to action

In a final step, this can lead to mobilization for concrete actions – from propaganda activities and logistical support to acts of violence (RAN 2022). „Armin O.,” for example, created and managed social media accounts for



IS fighters, while the perpetrators in Munich carried out violent attacks in 2024 and 2025 that were allegedly legitimized online by Islamist ideologies (Schüler 2017; Bavarian State Office of Criminal Investigation 2025).

RAN emphasizes that these phases do not necessarily occur in a fixed order and may overlap; moreover, individuals may „enter“ at different stages or abandon the process (RAN 2022). The case and interview data, as well as Schüler's findings, suggest that the transition from online to offline—i.e., from digital contacts to personal relationships—is a crucial tipping point at which prevention and intervention can be particularly effective (Schüler 2017).



5. Deradicalization and exit based on a German model – the role of the police

Bavaria's exit and disengagement work is part of the field of indicated prevention and is aimed at individuals who are already manifestly radicalized or at significant risk of radicalization (Schmidt 2018). It is essential to distinguish between deradicalization (cognitive change of attitude) and disengagement (cessation of behavior without necessarily renouncing the ideology) (Horgan 2008; Biene/Junk 2017).

5.1 Structural anchoring: Competence center for deradicalization

In Bavaria, statewide responsibility for the prevention of Islamist radicalization lies with the Competence Center for Deradicalization at the Bavarian State Criminal Police Office (BLKA) (Schmidt 2018). It is part of the „Bavarian Network for Prevention and Deradicalization against Salafism,“ in which general prevention (led by the Ministry of Social Affairs) and deradicalization (led by the Ministry of the Interior/Police) are organized on a division of labor basis (StMI/StMAS 2017).

- The Competence Center acts as a central coordination point for all security-related exit issues in Bavaria,
- a technical interface between the police, the Office for the Protection of the Constitution, the judiciary, youth and immigration authorities, and civil society organizations,
- and an operational unit with a multi-professional team (criminal investigators from the State Security Service, psychologists, Islamic scholars, social educators) (Schmidt 2018).

In order to cover the entire state, decentralized „deradicalization“ officers have been installed in all police headquarters to identify potential cases at an early stage and feed them into the support structure (Schmidt 2018).



5.2 Police tasks in the exit process

Schmidt describes three core roles for the police in exit work: risk assessment, case management, and access facilitation („door opener“ function) (Schmidt 2018).

Risk assessment and risk management

The police are responsible for assessing the security relevance of each individual case (threat to public safety, possible serious crimes) (Schmidt 2018). They use structured instruments such as RADAR-iTE, VERA-2R, or DyRiAS-Screener Islamism, but combine their results with case-analytical, biography-related assessments („internal logic“ of the course) and carry out concrete risk analyses (Pressman/Flockton 2012; BKA 2017; Schmidt 2018). In particular, the Competence Center uses operational case analysis, psychological behavior and problem analysis (S-O-R-C), and consistency theory considerations to balance risk and protective factors and identify windows of opportunity for intervention (Grawe 2004; Schmidt 2018).

Case coordination and interface with regulatory structures

In security-related cases, the BLKA Competence Center takes charge of case management and coordinates the youth welfare office, immigration authorities, prison services, schools, social services, and civil society organizations to avoid parallel, uncoordinated measures (Schmidt 2018). The police ensure clarity of roles (who is responsible for security, who for counseling, who for social-educational support) and continuous case monitoring throughout the entire process (Schmidt 2018).

Access to clients and motivational work

Initial contacts in the Islamist sphere often take place via the police or the Office for the Protection of the Constitution, because individuals rarely



come forward „voluntarily“ with a desire to leave (Schmidt 2018; Schüler 2017). Schmidt emphasizes the importance of early „boundary-setting conversations“: offers of discussion by the police in which legal boundaries and possible consequences are clearly stated and, at the same time, low-threshold counseling services (e.g., VPN) are provided (Schmidt 2018). In ambiguous cases where contact is not initiated at the request of the person concerned, motivational interviewing techniques are emphasized: structured cost-benefit reflection on remaining and leaving (Schmidt 2018).

5.3 Cooperation with civil society organizations

An „essential cornerstone“ of the Bavarian concept is the contractually regulated cooperation between the BLKA Competence Center and a civil society organization (Violence Prevention Network) (Schmidt 2018). The division of tasks is clear:

Police

- Hazard prevention, risk assessment, case coordination,
- involvement and information of other authorities,
- access provision (e.g., after preliminary investigations, information from institutions),
- Ensuring the safety of clients and counselors (Schmidt 2018).

Civil society organizations:

- Individual deradicalization and distancing counseling for those affected (ideological, affective, and pragmatic levels)
- counseling for relatives, coaching for institutions (schools, shelters, youth welfare services),
- outreach work and long-term support (Schmidt 2018; El Difraoui et al. 2021).



The author emphasizes the following as success factors for this cooperation: clear case responsibility, defined communication channels, coordinated handling of data protection, and mutual acceptance of the different roles (security authority vs. trusted authority) (Schmidt 2018).

5.4 The role of the police in light of Wolfgang Schüler's recommendations

Schüler qualitatively analyzes the radicalization and deradicalization processes of Islamist actors and derives concrete starting points for the police and security authorities (Schüler 2017). Key recommendations are:

Early, non-criminal intervention

Schüler uses several cases to show that early police intervention—even without any existing criminal offenses—can have a significant distancing effect if it combines setting boundaries with offering specialized counseling (Schüler 2017). At the same time, he warns against mixing repressive measures and preventive approaches by the same unit, as an approach perceived as purely punitive can tend to deepen radicalization (example P8) (Schüler 2017). From this, he derives the recommendation that approaches should be conducted via a „neutral“ police structure (e.g., a competence center, not an investigative state security agency) (Schüler 2017).

Using „periods of doubt“ as windows of opportunity for intervention

In his interviews, Schüler describes frequent phases of doubt, temporary distancing from the scene, or „timeouts“ during which those affected would have been open to discussion in retrospect (Schüler 2017). He recommends systematically using information about the scene provided by state security and constitutional protection agencies to identify such phases and make targeted and early offers of dialogue—ideally in conjunction with civilian organizations (Schüler 2017).



Special responsibility of the police in detention contexts

Schüler shows that solitary confinement can trigger distancing processes, but that the services offered in prisons often do not match the inmates' biographies and backgrounds (linguistically, religiously, milieu-specifically) (Schüler 2017). He recommends working with prison authorities and organizations to involve Muslim chaplains and credible defectors more closely, with the police and the Office for the Protection of the Constitution acting as interfaces for information and as partners in risk assessment (Schüler 2017).

Police as a catalyst for civil society resources

In cases of domestic violence in the Salafist milieu (e.g., P4, P9), the situation was handled by the police as a „normal“ victim protection case; Schüler recommends systematically referring to exit counseling (HAYAT, VPN, etc.) and publicizing the relevant contact channels in the police, youth welfare, and social services offices (Schüler 2017). Overall, Schüler thus reinforces the idea of the police as a catalyst and mediator between security agency hazard prevention and civil society deradicalization practices—a role that is institutionally implemented in the Bavarian Competence Center (Schmidt 2018).

5.5 Model-oriented practice: Pfundmair/Schmidt and psychological mechanisms

The contribution by Pfundmair and Schmidt combines a social-psychological model of radicalization and deradicalization with case work from the Competence Center (Pfundmair/Schmidt 2019). They distinguish between:

- individual processes (need for significance, loss of control, search for transcendence),
- group processes (integration into radical networks, group identity),



- catalyzing processes (desensitization, dehumanization, preparation for violence) (Pfundmair/Schmidt 2019).

Deradicalization is understood as „reversing the causes of radicalization“ on two levels (Garfinkel 2007; Laub/Sampson 2001; Pfundmair/Schmidt 2019).

Work on individual deprivation

In the cases of Ali H. and Mustafa R., the police and civil society organizations addressed issues such as loneliness, lack of family stability, lack of educational and career prospects, and the search for religious meaning (Pfundmair/Schmidt 2019). The police coordinated the cases, assessed security, and involved the youth court assistance service and the public prosecutor's office, while the civil society organization provided outreach counseling, worked with family members, and helped the young people establish new educational and career paths (Pfundmair/Schmidt 2019).

Creating new social environments

The case of Sarah F. in particular makes it clear that simply removing someone from an extremist environment without establishing stable alternative relationships and structures is doomed to failure (Pfundmair/Schmidt 2019). Only the second, coordinated intervention—with a return to Bavaria and close cooperation between the youth welfare office, the mother-and-child facility, civil society organizations, and the coordinating police department—led to a lasting distancing (Pfundmair/Schmidt 2019).

Pfundmair/Schmidt state that deradicalization—analogueous to the concept of desistance in criminology—is not a binary event, but rather a process that must be stabilized over the long term and that depends on ongoing cooperation between the police, academia, and civil society practitioners (Gadd/Farrall 2004; Pfundmair/Schmidt 2019).



5.6 Police and security authorities in the European context

The RAN's recommendations on tertiary prevention emphasize network-oriented, multidisciplinary cooperation in which security authorities play a clearly defined but limited role (RAN 2022). The police and domestic intelligence services should primarily carry out risk assessments, provide security-related information, and ensure the protection of clients and counselors without taking on ideological or therapeutic core work themselves (RAN 2022).

In this sense, the Bavarian approach with the BLKA's Center of Excellence for Deradicalization is in line with the RAN guidelines: the police focus on risk analysis, hazard prevention, and case management, while the actual deradicalization and disengagement work is carried out by a specialized civil society organization (Schmidt 2018; El Difraoui et al. 2021). The clear separation of roles between the security authorities' coordination office and the advisory organization, the involvement of youth welfare services, the prison system, immigration authorities, and schools in structured case conferences, and a joint, case-related risk and needs analysis are in line with the „case management“ approach described by RAN (RAN 2021).

RAN and the related German specialist concepts also emphasize that security authorities should not only include dangers to the general public in their assessments, but also threats to advisors, and take preventive protective measures if necessary (RAN 2022; El Difraoui et al. 2021). At the same time, the police and the Office for the Protection of the Constitution are seen as important knowledge partners who feed their scene-specific situation reports into the networks without claiming a „monopoly on the truth“ about radicalization processes (RAN 2022). This idea of a circular transfer of knowledge between practitioners, security authorities, and researchers is reflected, for example, in the Bavarian Competence Center's links to national and European exchange formats (Schmidt 2018; El Difraoui et al. 2021).



The recommendations developed by Wolfgang Schüler specify these RAN principles at the micro level of policing: Early, non-criminal proceedings approaches that clearly distinguish between investigative mandates and preventive dialogue, the systematic use of „phases of doubt“ as windows of opportunity for intervention, and the deliberate separation between state security services conducting investigations in a „ „ manner and „neutral“ contact structures correspond to the RAN model of „early, least intrusive, cooperative“ (Schüler 2017; RAN 2021).

In this way, the police do not become „deradicalizers“ in the exit process, but rather a security authority engine and catalyst that—in line with European recommendations—opens up access, manages risks, and networks, while cognitive and biographical change processes take place primarily in civil society and social education settings (Schmidt 2018; El Difraoui et al. 2021).



6. Summary

This article has shown that deradicalization and disengagement should be understood as multidimensional, processual phenomena that encompass ideological, emotional, and everyday life levels and cannot be captured in binary categories of „radical“ vs. „deradicalized“ (Horgan 2008; Pfundmair/Schmidt 2019). Model-oriented approaches that distinguish between individual, group-related, and catalytic factors of radicalization and conceive of deradicalization as a reversal of these processes offer a viable basis for the development and evaluation of intervention strategies (Pfundmair/Schmidt 2019).

In the Bavarian approach, the police—exemplified by the Competence Center for Deradicalization—are neither marginalized nor overburdened, but rather play a specific role in risk assessment, case coordination, and access management (Schmidt 2018). Above all, through early, boundary-setting and at the same time supportive approaches, the use of biographical intervention windows, the involvement of youth welfare services, the prison system and civil society organizations, and the protection of counselors, the police become the security authority driving force behind a network-oriented exit system (Schüler 2017). In a successful, nationwide exit program, the police are therefore more of a driving force than a passenger.

The recommendations of the research (Pfundmair/Schmidt, Schüler) and the European guidelines of the Radicalisation Awareness Network are largely parallel: they call for a clear separation of roles, multidisciplinary case conferences, early, proportionate interventions, and a mutual transfer of knowledge between security authorities, practitioners, and academia (RAN 2018; El Difraoui/Trautmann/Wiedl 2021). Against this backdrop, the Bavarian approach can be seen as an exemplary implementation of a RAN-compatible model in which the police use their genuine powers—to professionally ensure security and to network actors—in the service of sustainable distancing and deradicalization processes (Schmidt 2018; Pfundmair/Schmidt 2019).



7. Bibliography

Abou-Taam, M. (2014): Salafism in Germany – A Challenge for Democracy. *Journal of International Criminal Law*, 9(9), 442–449.

Abou-Taam, M., Gerlach, R., & Ruf, M. (2016): *Salafism in Germany – Causes, Dynamics, Recommendations for Action*. Wiesbaden: Springer VS.

Akram, M. & Nasar, A. (2023): Systematic Review of Radicalization through Social Media. *Ege Academic Review*, 23(2), 279–296.

Bauknecht, B. R. (2018): Salafism – A Variation of Islamism. In: El Di-fraoui, A., Trautmann, C., & Wiedl, N. (Eds.), *Deradicalization and distancing work. Companion book to the qualification course on counseling in the field of Islamist-based extremism* (pp. 13–18). Nuremberg: BAMF.

Berger, J. M. & Morgan, J. (2015): *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*. Washington, DC: Brookings Institution.

BfV – Federal Office for the Protection of the Constitution (2012): *Salafism in Germany – Manifestations and dangers*. Cologne.

BfV – Federal Office for the Protection of the Constitution (2017): *2016 Report on the Protection of the Constitution*. Berlin.

Biene, J. & Junk, J. (2017): What works? Deradicalization in theory and practice. In: El-Mafaalani, A., Toprak, A. & Worbs, S. (Eds.), *Deradicalization. Scientific perspectives and practical experiences* (pp. 95–120). Bonn: bpb.

Borum, R. (2011): Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, 4(4), 7–36.

Conway, M. (2006): Terrorism and the Internet: New media – new threat? *Parliamentary Affairs*, 59(2), 283–298.

Conway, M., Scrivens, R., & Macnair, L. (2019): *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends*. ICCT



Policy Brief. The Hague: International Centre for Counter-Terrorism.

Dantschke, C. & Kiefer, M. (2013): Ways out of extremism – exit programs in the field of Islamism. In: Ceylan, R. & Kiefer, M. (Eds.), *Salafism – Fundamentalist movements and radicalization prevention* (pp. 93–110). Wiesbaden: Springer VS.

Doosje, B. et al. (2016): Terrorism, Radicalization, and Deradicalization. *Current Opinion in Psychology*, 11, 79–84.

El Difraoui, A., Trautmann, C., & Wiedl, N. (Eds.) (2021): *Deradicalization and distancing work. Companion book to the qualification course on counseling in the field of Islamist-based extremism (Contributions to Migration and Integration, Volume 9)*. Nuremberg: Federal Office for Migration and Refugees.

El-Mafaalani, A., Toprak, A., & Worbs, S. (Eds.) (2016): *Deradicalization. Scientific perspectives and practical experiences*. Bonn: Federal Agency for Civic Education.

Europol (2023): *Online gaming platforms, live streaming, and extremism*. The Hague: Europol Trend Report.

Gadd, D. & Farrall, S. (2004): Criminal careers, desistance and subjectivity: Interpreting men's narratives of change. *Theoretical Criminology*, 8(2), 123–156.

Garfinkel, R. (2007): *Personal Transformations: Moving from Violence to Peace*. Washington, DC: United States Institute of Peace.

Gill, P. et al. (2017): *The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for progressing research*. National Institute of Justice, Final Report.

Grawe, K. (2004): *Neuropsychotherapy*. Göttingen: Hogrefe.

Horgan, J. (2008): *Deradicalization or Disengagement? A Process in Need of Clarity and a Counterterrorism Initiative in Need of Evaluation*. *Perspectives on Terrorism*, 2(4), 3–8.



- Klausen, J. (2015): Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1–22.
- Laub, J. H. & Sampson, R. J. (2001): Understanding Desistance from Crime. *Crime and Justice*, 28, 1–69.
- Moghaddam, F. M. (2005): The Staircase to Terrorism: A Psychological Exploration. *American Psychologist*, 60(2), 161–169.
- Neumann, P. R. (2016): *Terror is among us. Jihadism and radicalization in Europe*. Berlin: Ullstein.
- Pfahl-Traughber, A. (2019): *Islamist extremism. Manifestations, causes, countermeasures*. Bonn: bpb.
- Pfundmair, M. (2018): Ostracism promotes a terroristic mindset. *Behavioral Sciences of Terrorism and Political Aggression*.
- Pfundmair, M. & Schmidt, H. (2019): The path to radicalization and back: Deradicalization and its psychological mechanisms in practice. Unpublished manuscript, University of Ulm/Bavarian State Criminal Police Office.
- Pressman, E. & Flockton, J. (2012): Calibrating Risk for Violent Political Extremism: The VERA 2 Structured Assessment. *The British Journal of Forensic Practice*, 14(4), 237–251.
- RAN – Radicalization Awareness Network (2018): *RAN Activities in Communication & Narratives*. Amsterdam: RAN Centre of Excellence.
- RAN – Radicalisation Awareness Network (2021): *RAN C&N: RAN guidelines for effective alternative and counter-narrative campaigns (GAMMMA+)*. Amsterdam: RAN Centre of Excellence.
- RAN – Radicalisation Awareness Network (2022): *Online Radicalisation – What We Know*. Amsterdam: RAN Centre of Excellence.
- Roy, O. (2003): EuroIslam: The Jihad Within? *The National Interest*, 71, 63–73.



Sageman, M. (2004): *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Schmidt, H. (2018): *Indicated Prevention: Goals, Target Groups, and Approaches in the Field of Politically Motivated Radicalization*. In: El-Maafaalani, A., Toprak, A., & Worbs, S. (Eds.), *Deradicalization: Scientific Perspectives and Practical Experiences* (pp. 203–224). Bonn: bpb.

Schüler, W. (2017): *Radicalization and Deradicalization of Islamists. A Qualitative Analysis of Case Files and Expert Interviews from the Competence Center for Deradicalization of the Bavarian State Criminal Police Office*. Unpublished master's thesis, University of Public Service in Bavaria.

StMI/StMAS (2017): *Bavarian Network for Prevention and Deradicalization against Salafism*. Munich: Bavarian State Ministry of the Interior / Bavarian State Ministry of Labor and Social Affairs.

Whittaker, J. (2022): *Online Radicalization: What We Know*. In: RAN Centre of Excellence (ed.), *Online Radicalization – What We Know* (background paper). Amsterdam: RAN.



References

- 1) https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=OJ:L_202502611
- 2) [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765777/EPRS_STU\(2025\)765777_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765777/EPRS_STU(2025)765777_EN.pdf)
- 3) https://sieps.se/media/qedbmd5f/2025_6epa.pdf
- 4) (The Facilitation Proposal: Assessing the EU's response to the smuggling of migrants Gabriella Sanchez)
- 5) <https://eucrim.eu/news/edps-raises-concerns-over-planned-police-cooperation-in-migrant-smuggling/>
- 6) https://protectnotsurveil.eu/uploads/ProtectNotSurveil-Europol_Paper.pdf - A position paper on the European Commission's proposal for a Regulation to enhance Europol's support in 'preventing and fighting migrant smuggling' STOPPING THE UNFETTERED EXPANSION OF EUROPOL'S DIGITAL SURVEILLANCE POWERS AGAINST MIGRANTS
- 7) <https://www.europol.europa.eu/about-europol/european-serious-and-organised-crime-centre-esocc/european-migrant-smuggling-centre-emsc>

This analytical article has been developed as part of the project "Capacity building through exchange of good practices and research in the security domain" No. BG65ISPR001-3.004-0002, Contract No. 812108-68-02.10.2024, funded by the Program of the Republic of Bulgaria under the Internal Security Fund 2021-2027.

The content of this material does not reflect the official opinion of the European Union and the Responsible Managing Authority. Responsibility for the information and views expressed in the document lies with its author and the European Institute Foundation.



Co-funded by
the European Union

EUROPOL'S ENHANCED ROLE IN COMBATING MIGRANT SMUGGLING AND HUMAN TRAFFICKING

Nadya Dimitrova



Introduction

In a global context, efforts to combat migrant smuggling are widely regarded as an essential component of national migration management strategies. This approach is often based on the understanding that organised smuggling networks should be identified, disrupted and neutralised in order to protect migrants from exploitation and reduce irregular migration.

Preventing and combating migrant smuggling and human trafficking are among the European Union's key priorities and are crucial for efficient management of irregular migration. Criminal networks exploit people's vulnerability and desperation, using land, sea, and air routes to facilitate illegal crossing of state borders. These activities not only endanger migrants' lives and safety but are also driven by the goal of maximizing profits for the perpetrators.

The majority of people who cross the EU's external borders irregularly do so with the assistance of migrant smugglers. Although it is often assumed that migrants consent to being smuggled, they remain exposed to significant risks, including the danger of becoming victims of human trafficking. The defining purpose of human trafficking is the exploitation of victims. Both migrant smuggling and human trafficking are considered criminal offences under the EU law, and in both cases, perpetrators act to obtain financial or other material benefit.

The EU's Legislative Framework and New Initiatives

In November 2023, the European Commission presented a legislative proposal to update and strengthen the European Union's framework for combating migrant smuggling, known as the "Facilitators Package." The existing framework, adopted in 2002, established a general definition of the criminal offence of "facilitating unauthorized entry, transit and residence," as well as a criminal law mechanism aimed at preventing and penalising such conduct.



In December 2024, the Council of the European Union reached a general approach on the proposal, introducing a modernised EU criminal law instrument. The new framework aims to clearly define and effectively sanction organised criminal networks involved in migrant smuggling, align penalties with the seriousness of the offences, expand jurisdictional scope, strengthen Member States' capacities for prevention and enforcement, and improve data collection and reporting.

The proposal grants Member States considerable discretion in defining and penalising the offence of “smuggling.” Although the text includes a humanitarian clause — for example, assistance provided to close family members or support offered on humanitarian grounds — and explicitly states that migrants should not be prosecuted solely for having been the object of smuggling, national authorities retain broad discretionary powers. This includes the possibility for courts to impose sanctions in accordance with national law.

In this context, it is important to note that the United Nations Office on Drugs and Crime (UNODC), the depositary of the Protocol Against the Smuggling of Migrants, has repeatedly expressed concern about divergences between national and regional definitions and the objectives and spirit of the Protocol.

Strengthening Europol's Role

The general objective of the legislative proposal, which became a Regulation in December 2025, was to strengthen Europol's role in combating migrant smuggling and human trafficking, particularly through reinforcing the European Centre Against Migrant Smuggling.

The Regulation modernises cooperation between Member States and Europol by establishing a harmonised legal and technical framework, introducing mandatory real-time information exchange, and clarifying coordination mechanisms. Europol is granted expanded powers, including



the ability to support and initiate cross-border operations, deploy expert teams, and provide strategic and operational analyses aimed at dismantling criminal networks, their financial flows, and logistical infrastructure.

The Regulation also enhances operational capacity through joint training programmes, formalised operational protocols, and targeted EU funding for technology and human resources. In light of the systematic exploitation of legal and operational loopholes by trafficking networks, the initiative highlights the need for a coordinated European response while emphasising the protection of fundamental rights, the role of civil society, and the importance of transparency and accountability in implementing the new measures.

Overall, the Regulation expands Europol's operational powers, facilitates more efficient data exchange, and enables faster and better-coordinated cross-border action.

Purpose and Content of the Regulation

Regulation (EU) 2025/2611, amending Regulation (EU) 2016/794, was adopted on 16 December 2025 with the aim of strengthening Europol's capacity to prevent, detect, and investigate the illegal transfer of migrants and human trafficking. The Regulation expands Europol's support to Member States in operational, analytical, technical, and forensic matters, provides for the establishment and reinforcement of specialised Union centres of expertise, and clarifies the mechanisms for cross-border information exchange, including through the SIENA system and the network of immigration liaison officers.

The Regulation was published in the Official Journal of the European Union in December 2025, marking a significant step towards a more integrated and effective European approach to combating two of the gravest forms of cross-border organised crime.

More broadly, the Regulation updates the legal framework governing the activities of Europol — the European Union Agency for Law Enforcement



Cooperation. Its primary objective is to enhance cooperation and coordination among Member States in addressing two of the most serious forms of transnational organised crime:

- the smuggling (illegal transfer) of migrants; and
- trafficking in human beings.

Due to their inherently cross-border nature, these crimes often exceed the capacity of individual Member States to address them effectively on their own, thereby necessitating a strengthened pan-European approach and a more active role for Europol.

Migrant smuggling and trafficking in human beings - two different crimes

The term “migrant smuggling” is often confused with, or used interchangeably with, “trafficking in human beings” even though they refer to different criminal offences.

Migrant smuggling is generally defined as facilitating the illegal entry of a person into a country other than their own in exchange for financial or material benefit.

Trafficking in human beings, by contrast, involves the recruitment, transportation, transfer, harbouring, or receipt of persons through the use of force, fraud, coercion, or abuse of vulnerability for the purpose of exploitation and profit.

Several key distinctions exist between the two crimes. Migrant smuggling necessarily involves the crossing of national borders, whereas trafficking in human beings may occur both within a single country and across borders. The United Nations Office on Drugs and Crime (UNODC) Protocol Against the Smuggling of Migrants treats migrants as the object of smuggling and the act itself as a crime against the state rather than against the individual. In contrast, the UNODC Protocol to Prevent, Suppress and Punish Trafficking in Persons defines human trafficking as a crime against the individual.

Nevertheless, although smuggled migrants are not considered “victims” of the



crime of smuggling itself, they may become victims of other offences during the smuggling process, including sexual and physical violence, abduction, theft, murder, manslaughter, and even human trafficking.

In practice, migrant smuggling and trafficking in human beings may overlap and occur simultaneously in the broader context of irregular migration. For example, a person who voluntarily engages the services of a smuggling facilitator may subsequently fall into a trafficking situation when, during transit, they are forced to work — often in criminal activities — in order to repay additional expenses not included in the original agreement. Conversely, victims of trafficking may find themselves compelled to rely on smuggling facilitators as the only available means of leaving, transiting through, or entering another country.

Research further indicates that young people and children attempting to reach destinations within the EU who voluntarily engage smugglers are sometimes offered, and may accept, reduced fees in exchange for steering vessels or driving vehicles. For many, taking control of a boat or vehicle is perceived as a means of safeguarding both their own lives and the lives of others on board.

Although the Protocol Against the Smuggling of Migrants stipulates that individuals should not be criminalised solely for having been the object of smuggling, several EU countries have systematically brought charges against smuggled migrants, including unaccompanied minors, for facilitating smuggling operations.

In this context, the Regulation should not be viewed as an isolated legislative act, but rather as a natural continuation and further development of the European Union's broader efforts to strengthen operational cooperation in combating cross-border organised crime. Beyond defining Europol's expanded role and the mechanisms for supporting Member States, the Regulation also illustrates how these tools operate at both political and institutional levels. It is within this broader framework that the Regulation's principal achievements should be assessed, together with its significance for the development of a coherent, coordinated, and sustainable European approach to combating the illegal transfer of migrants and trafficking in human beings.



What this Regulation Achieves

The Regulation strengthens EU-level coordination in the fight against the illegal transfer of migrants and trafficking in human beings, without affecting or altering migration and asylum policies. Rather, it reinforces Europol's role as a central coordination mechanism for operational and analytical cooperation among Member States, while leaving the powers of national law enforcement authorities unchanged.

The Regulation also reflects a clear policy choice to address these crimes primarily through enhanced cooperation in the fields of security and law enforcement, rather than through further harmonisation of national criminal law systems..

Significance of the Regulation at Policy Level

At the policy level, the Regulation recognises that networks involved in the illegal transfer of migrants and human trafficking operate across national borders and therefore require sustainable, permanent coordination structures at EU level. In this regard, it provides a stable institutional solution by establishing a permanent specialised centre within Europol, replacing previous temporary and ad hoc cooperation mechanisms.

At the same time, the Regulation builds on and strengthens existing EU instruments and frameworks, such as the European Multidisciplinary Platform Against Criminal Threats (EMPACT), rather than creating new parallel structures. In doing so, it contributes to greater efficiency, coherence, and institutional resilience within the EU's security policy framework.

Key Policy Compromises

The Regulation reflects a series of deliberate policy compromises that seek to balance enhanced law enforcement effectiveness with the protection of fundamental rights.



First, it introduces stronger EU-level coordination among law enforcement authorities, which inevitably raises concerns regarding personal data protection and compliance with fundamental rights safeguards.

Second, the Regulation reinforces an approach primarily driven by internal security considerations, focusing on operational countermeasures against criminal networks, rather than addressing the broader structural root causes of irregular migration.

Third, the accelerated exchange of intelligence and operational information between Member States and Europol highlights the need to balance the effectiveness of cross-border cooperation with the preservation of national control over sensitive data and operational decision-making.

Key Policy Conclusion

In summary, the Regulation represents a gradual yet strategically significant enhancement of internal security governance in the European Union. It introduces a higher degree of coordination, more intensive data sharing and strengthened EU-level capacity, without leading to formal centralisation of police powers. In this way, the Regulation outlines a model of “integrated yet decentralised” security that is likely to continue shaping the European policies in this area in the future as well.

These political compromises find concrete expression not only at the level of objectives and priorities, but also in the very legal structure of the Regulation. The balance between enhanced law enforcement coordination and the protection of fundamental rights, between the efficiency of cross-border cooperation and the preservation of national sovereignty, has materialized precisely through the amendments to the Europol Regulation. Therefore, an analysis of the legal implications of the new framework is key to understanding the Regulation’s actual scope and limitations.



What Has Changed in Legal Terms

The Regulation amends Regulation (EU) 2016/794 (the Europol Regulation) by updating the legal framework governing the Agency's mandate and activities. It expands the tasks assigned to Europol regarding the prevention, detection and support of investigations related to the illegal transfer of migrants and human trafficking. In this context, the Regulation formalises the establishment of a permanent specialised centre within Europol and broadens the scope of lawful data processing for specific purposes directly linked to the fight against serious and organised crime.

Key Legal Highlights

Despite its extended mandate, Europol retains its status as a supporting rather than an executive body. The Agency has no authority to make arrests or enforce coercive measures, as operational activities remain entirely within the competence of national authorities.

Europol's processing of data should continue to be in full compliance with the Europol Regulation, the applicable European Union data protection law and the Charter of Fundamental Rights of the European Union. Member States retain full responsibility for conducting investigations and prosecutions, as well as for the way in which intelligence and analytical information provided by Europol is used under national proceedings.

Areas of Legal Sensitivity

Alongside the safeguards it provides, the Regulation raises a number of issues of increased legal sensitivity. Among these, the principles of proportionality and necessity stand out in the context of extended use and sharing of data, as does the efficient oversight of the processing of biometric and cross-border data.

Particular attention is drawn to the risk of so-called “function creep” in



intelligence-led policing, whereby initially limited powers may gradually expand beyond their original scope. Furthermore, the lack of a full impact assessment by the European Commission — a circumstance frequently noted by legal analysts — reinforces the need of follow-up monitoring and critical evaluation of the Regulation's practical implementation.

What This Means for Operational Law Enforcement Agencies, Analysts and Coordinators

What has changed in reality

The implementation of the Regulation reinforces Europol as a more active and integrated operational partner, particularly in cases with a clear cross-border dimension. The exchange of information between national authorities and Europol is expected to become faster, more systematic and more comprehensive, reducing fragmentation and delays in data sharing.

The newly established permanent specialised centre within Europol consolidates expertise and operational capacity by bringing together specialised analysts, producing centralised intelligence outputs and providing structured support for operational coordination among participating Member States.

What the Achievement Is for Law Enforcement Agencies

For national law enforcement agencies, the Regulation creates conditions for a better-quality, coherent intelligence picture, enabling the consolidation of data and cases from different Member States. This results in stronger support for joint operations and multinational task forces, as well as clearer and formalised channels for coordination with other key EU agencies, including Frontex, Eurojust and relevant operational networks.

At the same time, it reduces reliance on temporary, ad hoc or informal structures for cooperation, thereby increasing the predictability and sustainability of operational interactions.



What Remains Unchanged

Despite Europol's enhanced role, national authorities retain full operational sovereignty. They continue to lead investigations, determine operational tactics, and carry out arrests and prosecutions. Europol maintains a supporting and coordinating role without assuming control over national operational activities.

Operational Conclusion

From an operational perspective, the Regulation aims to make cross-border cooperation smoother, more predictable and more structured. For teams working on cross-border cases, Europol is meant to be a “default” partner rather than an additional or elective option, which fundamentally shifts the practical logic of joint work within the EU.

Examples of Typical Cases with the Greatest Operational Impact

1. Multinational smuggling networks along major migration routes

In cases where organised criminal groups operate simultaneously in several Member States — e.g. along the Western Balkan, Central Mediterranean or Eastern Mediterranean routes — the new framework enables Europol to consolidate operational and intelligence information from various national sources into a single analytical snapshot. This facilitates the identification of key organisers, logistical intermediaries and financial flows, which often go unnoticed in isolated national investigations.

2. Cases involving links between migrant smuggling and human trafficking

Whenever an initial investigation into illegal transfer of migrants reveals elements of exploitation — such as labour or sexual exploitation after arrival — the permanent specialised centre at Europol can ensure a rapid analytical transition between the two types of crimes. This allows for a



timely referral of the investigation, better protection of potential victims and more efficient use of existing tools against human trafficking.

3. Investigations involving digital platforms and social networks

Smuggling networks are increasingly using encrypted messaging apps, social media and online platforms to recruit clients, coordinate routes, and handle payments. In such cases, Europol can provide specialised expertise in digital investigations, analysis of communication patterns and links between online and offline activities, assisting national authorities to connect digital evidence from different jurisdictions.

4. Joint operations involving several EU agencies

In complex operations involving border control, criminal investigations and judicial coordination, the new framework facilitates closer cooperation among Europol, Frontex and Eurojust. A typical example includes operations targeting networks that facilitate illegal crossings using forged documents or misuse of visa procedures, which require simultaneous operational, legal and analytical support.

5. Rapidly evolving cases demanding operational urgency

In situations where there is an immediate risk to the life and health of migrants — such as dangerous sea crossings or detention of individuals with the purpose of extortion — the enhanced and formalised information sharing with Europol enables a faster cross-border response. The centralised coordination facilitates aligned actions among Member States and reduces the time required for operational decision-making.



Europol's Role and Tasks

Before 2026 (Regulation 2016/794)

- Europol assisted national law enforcement authorities by facilitating cooperation and information exchange in cases involving serious cross-border crime and terrorism.
- The Agency's tasks were primarily analytical and coordinative — e.g. analysing data, preparing threat assessments and maintaining criminal records.
- Europol could support operational activities, but only indirectly and without a formal role in specific areas of crime such as illegal transfer of migrants.
- Europol's focus was on supporting Member States' investigations, not on leading operations.

Key finding: Europol primarily functioned as a coordination and analytical centre, rather than as an operational law enforcement service.

After 2026 (Regulation 2025/2611)

- Europol's mandate is being expanded to explicitly include support in cases of illegal transfer of migrants and human trafficking.
- The Agency can now coordinate, organise and help investigative and operational activities in support of Member States, including:
 - o establishment of joint investigation teams;
 - o involvement in operational task forces;
 - o deployment of Europol staff in Member States.
- This goes beyond purely analytical work and includes more active operational support, while remaining within the legal limits.
- Europol is granted formal responsibility to support cross-border information exchange and the coordination of investigations in these specific areas of crime.



Information Exchange

Before 2026

- The exchange of information between Member States and Europol was voluntary and focused on general criminal intelligence information.
- There were no explicit requirements for Member States to share certain types of data (e.g. from operational task forces or immigration liaison officers) with Europol.

After 2026

- Member States are required to share information with Europol regarding illegal transfer of migrants and human trafficking, including:
 - data from immigration liaison officers in third countries;
 - operational information from joint activities and cooperation frameworks.
- The purpose is to reduce gaps and delays in the flow of data that could undermine the efficiency of cross-border investigations.

Key finding: The post-2026 Regulation shifts Europol from primarily an analytical support centre into a more active and structurally coordinating partner, with clearly defined obligations and responsibilities for information exchange in the field of migration-related crime.

Establishment of a Permanent Centre

Before 2026

- There was no specialised centre within Europol focused on the issue of illegal transfer of migrants and human trafficking.
- Europol had other specialised units (such as the European Cybercrime Centre), but there was no structure dedicated specifically to migrant smuggling.



Key finding: The approach so far was based on ad hoc working groups and analytical support, without established permanent expertise.

After 2026

- The Regulation establishes the European Centre Against Migrant Smuggling (ECAMS) as a permanent structure within Europol.
- The Centre's main functions include:
 - providing strategic, operational and technical support to national authorities;
 - coordination of actions with the Member States;
 - interaction and cooperation with other EU agencies such as Frontex and Eurojust.
- The purpose is to build sustainable expertise and structured processes that replace the ad hoc approach with permanent and predictable mechanisms.

Use of Data and Analytics

Before 2026

- Europol was authorised to process data necessary for the performance of its core functions, but the processing of biometric data (such as fingerprints and facial recognition data) was limited and was not specifically targeted at cases of migrant smuggling.
- Data sharing and use were governed by the general provisions of the Europol Regulation and EU data protection law.

After 2026

- Europol is expressly authorised to process biometric data to support the fight against migrant smuggling and human trafficking, subject to safeguards for:
 - necessity and proportionality;
 - protection of personal data and fundamental rights;
 - compliance with EU security and confidentiality standards.



- The updated Regulation emphasises enhanced analytical tools and resources that support prevention, investigations and coordination among Member States.

Key finding: The establishment of a permanent specialised centre and the expansion of data-processing capabilities transform Europol into a more structured and effective partner in cross-border investigations, while maintaining obligations under fundamental rights and data protection frameworks.

Coordination and support to Member States

Before 2026

- Europol supported Member States through:
 - strategic analyses;
 - threat assessment;
 - coordination platforms such as SIENA.
- The Agency had no formal authority to assign tasks or lead operations in specific areas of crime, such as migrant smuggling or human trafficking.

Key finding: Europol served primarily as an analytical and coordinating partner, without playing an active role in operational planning.

After 2026

- Europol's support is being expanded to include active structuring and coordination of operational efforts against migrant smuggling and human trafficking.
- Europol can now provide:
 - operational and technical support;
 - forensic expertise;
 - financial support for joint activities and cross-border operations.
- This means that Europol no longer merely analyzes and advises, but also supports the practical conduct of investigations and the coordination among Member States.



Key finding: The post-2026 Regulation transforms Europol into a more active and structurally integrated partner in cross-border operations, while maintaining national control over the running of investigations.

Summary of Europol-related amendments

DIMENSION	BEFORE REGULATION 2025/2611	AFTER REGULATION 2025/2611
Europol mandate	Broad support in serious cross-border crime and terrorism cases	Explicit mandate to support the fight against migrant smuggling and human trafficking
Operational role	Primarily analytical and coordination-based	More active operational support, within clearly defined legal limits
Information exchange	Voluntary and of general nature	Improved, structured and mandatory for certain types of data
Specialised centre	No specific centre	Establishment of a permanent European Centre Against Migrant Smuggling (ECAMS)
Processing of biometric data	Limited, not specifically targeted at migrant smuggling	Extended, with data protection safeguards (necessity, proportionality, compliance with EU standards)
Nature of support functions	Strategic and coordinating	Strategic, operational, technical & forensic support



What remains unchanged

- Europol still cannot **make arrests** or enforce the law — this role remains entirely with the Member States.
- **Data protection and fundamental rights:** all data processing activities are governed by data protection principles and the EU Charter of Fundamental Rights.
- **Responsibility for criminal prosecution:** Member States will continue to conduct investigations, press charges and lead court proceedings.

Key finding: Regulation 2025/2611 strengthens Europol's capacity for co-ordination, operational support and information exchange in cross-border cases of smuggling and trafficking, while preserving national control and safeguards for human rights.

Conclusion

The new Regulation, which in its final version also takes into account the concerns of civil society organisations, is a measured and balanced response to the need for more effective operational tools for Europol in the context of increasing cross-border threats. The legislator has deliberately retained the existing strict data protection framework, including the one concerning biometric data, without weakening the existing safeguards and even introducing additional precautionary mechanisms. The text of the Regulation does not alter the protection standards that the Agency is required to comply with. Instead, it provides additional resources and tools while maintaining existing oversight and control.

Overall, the Regulation can be evaluated as a reasonable compromise of two key objectives: on the one hand, strengthening Europol's operational capacity as a strong EU law enforcement agency, and on the other, ensuring a high level of protection for personal data and fundamental rights. It



is precisely this balance that will be crucial in the reform's practical implementation and public legitimacy.

Regulation 2025/2611 represents a strategic upgrade of Europol's capacity:

- a more structured and active role in cross-border operations against migrant smuggling and human trafficking;
- faster, mandatory and systematised exchange of information;
- permanent expertise through the European Centre Against Migrant Smuggling;
- increased capacity for data processing and analytical support, with safeguards for human rights protection.

At the same time, the **national control** over investigations, criminal prosecutions and arrest powers has been preserved. Europol thus becomes a key, reliable and integrated partner to the Member States in the fight against cross-border crime.



References

- 1) https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=OJ:L_202502611
- 2) [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765777/EPRS_STU\(2025\)765777_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765777/EPRS_STU(2025)765777_EN.pdf)
- 3) https://sieps.se/media/qedbmd5f/2025_6epa.pdf
- 4) (The Facilitation Proposal: Assessing the EU's response to the smuggling of migrants Gabriella Sanchez)
- 5) <https://eucrim.eu/news/edps-raises-concerns-over-planned-police-cooperation-in-migrant-smuggling/>
- 6) https://protectnotsurveil.eu/uploads/ProtectNotSurveil-Europol_Paper.pdf
- A position paper on the European Commission's proposal for a Regulation to enhance Europol's support in 'preventing and fighting migrant smuggling'
STOPPING THE UNFETTERED EXPANSION OF EUROPOL'S DIGITAL SURVEILLANCE POWERS AGAINST MIGRANTS
- 7) <https://www.europol.europa.eu/about-europol/european-serious-and-organised-crime-centre-esocc/european-migrant-smuggling-centre-emsc>



TECHNOLOGY-FACILITATED TRAFFICKING IN HUMAN BEINGS: EMERGING RISKS, INSTITUTIONAL RESPONSES AND POLICY CHALLENGES

Antoaneta Vassileva



1. Introduction

Trafficking in human beings is widely recognised today as one of the most serious and profitable forms of organised crime, ranking alongside drug and arms trafficking, with estimated annual profits reaching approximately €31 billion annually. For many years, numerous states denied the existence of modern forms of slavery or underestimated their consequences. Today, however, more than 180 countries worldwide acknowledge trafficking in human beings as a systemic problem and have adopted legislative measures aimed at its criminalisation and prevention.

Despite these efforts, trafficking in human beings for various forms of exploitation continues to thrive, including sexual exploitation, labour exploitation, forced criminality and, in some cases, organ removal. It influences migration dynamics, raises renewed security concerns within the European Union, and produces severe economic and social consequences for victims. The evolving nature of the crime increasingly challenges traditional responses, as trafficking operates across borders, sectors and legal frameworks, often exploiting regulatory and institutional gaps.

The rapid development and widespread use of information and communication technologies—particularly the Internet—have introduced a new dimension to trafficking in human beings. Digital technologies affect all stages of the crime, from recruitment and exploitation to control, prevention and counteraction. While the Internet provides fast, accessible and low-cost means of communication regardless of geographical location, over the past fifteen years it has also demonstrated its capacity to facilitate criminal activities in unprecedented ways.

Today, traffickers have access to highly efficient, often anonymous and largely unregulated digital tools that enable targeted recruitment, exploitation and control of victims at scale. Online environments offer traffickers unprecedented opportunities, which have been rapidly exploited. The commercial sex industry and individual users increasingly rely on digital platforms to recruit, advertise and exploit women and children. Similarly,



employment agencies, marriage services and modelling agencies are frequently misused to lure potential victims of modern forms of exploitation.

Chat rooms, specialised websites, encrypted communication channels and, in some cases, the so-called are used to identify and recruit victims, significantly increasing the exposure of children and young people to exploitation and amplifying existing vulnerabilities. Digital environments not only expand the scale of potential victimisation but also create new forms of vulnerability linked to online behaviour, visibility and interaction patterns. These dynamics not only reshape the profiles of traffickers and victims but also transform the *modus operandi* of trafficking networks, while simultaneously complicating detection, investigation and victim protection efforts.

In response, international and European legal and policy frameworks have progressively acknowledged the role of technology in facilitating trafficking in human beings. However, a growing gap persists between regulatory responses and operational realities. Institutional practices, investigative tools and victim support systems often struggle to adapt to forms of exploitation that are decentralised, transnational and mediated through digital environments. As a result, technology-facilitated trafficking frequently remains under-identified, under-investigated and insufficiently addressed within existing protection mechanisms.

This article examines how digitalisation reshapes trafficking in human beings by transforming the profiles of traffickers and victims, altering *modus operandi*, and challenging institutional responses, while also generating and amplifying new and existing vulnerabilities to exploitation in digital environments. Drawing on expert-based qualitative analysis informed by policy monitoring, institutional engagement and practical experience, the article highlights key challenges in detection, identification and victim protection in technology-facilitated trafficking cases. It further explores emerging global trends and promising practices before outlining policy-relevant recommendations aimed at strengthening coordinated, adaptive and victim-centred responses in an increasingly digitalised environment.



2. Conceptual and Legal Framework

Trafficking in human beings is defined under international law as a process involving the recruitment, transportation, transfer, harbouring or receipt of persons, by means of threat, force, coercion, deception or abuse of power, for the purpose of exploitation. While these core elements remain unchanged, the environments in which trafficking occurs have evolved significantly, particularly through the integration of digital technologies into all stages of the crime.

The increasing use of digital technologies in trafficking, however, should be understood within the broader process of digitalisation, which extends beyond the mere adoption of technical tools. Digitalisation refers to the systemic integration of digital technologies into social, economic and institutional processes, reshaping how interactions take place, how services are organised and how activities are coordinated across borders. It encompasses not only the Internet and digital communication tools, but also the growing reliance on online platforms, data-driven systems, automated processes and digital infrastructures in everyday life. As such, digitalisation reflects deeper structural transformations affecting power relations, access to information, and the organisation of labour and markets, with direct implications for how traffickers operate, how victims are recruited, controlled and exploited, and how law enforcement authorities detect, investigate and respond to trafficking-related crimes.

In the context of trafficking in human beings, digitalisation should not be understood as the emergence of a new form of crime, but rather as a cross-cutting enabler that reshapes how existing criminal conduct is carried out. Online platforms, social media, messaging applications and digital payment systems increasingly mediate recruitment, communication, control and exploitation. As a result, trafficking activities are often less visible, more decentralised and harder to detect through traditional investigative and regulatory approaches.



International and European legal frameworks have progressively acknowledged the role of technology in facilitating trafficking-related crimes. Instruments such as the Council of Europe Convention on Action against Trafficking in Human Beings and relevant European Union directives provide a comprehensive definition of trafficking and establish obligations related to prevention, victim protection and prosecution. More recent policy documents and strategies increasingly reference online recruitment, digital facilitation and the need for enhanced cooperation with technology actors.

At the European level, the legal and policy landscape addressing online harms to children and platform responsibility has also evolved significantly, with important implications for trafficking-related exploitation. Instruments such as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention), alongside EU legislation targeting child sexual abuse material (CSAM), establish obligations related to prevention, detection and victim protection in digital environments². More recently, the EU Digital Services Act has introduced horizontal rules on platform accountability, risk assessment and content moderation, including with regard to systemic risks affecting fundamental rights. In parallel, the proposed Regulation laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final) reflects ongoing efforts to strengthen detection and reporting mechanisms for online sexual exploitation. While these frameworks are not trafficking-specific, they increasingly shape the regulatory environment in which technology-facilitated exploitation occurs, particularly in cases involving children and platform-mediated abuse.

However, despite this growing recognition of the role of digital technologies in facilitating trafficking-related activities, existing frameworks largely remain technology-neutral in their operational design. Legal definitions focus on acts, means and purposes, but offer limited guidance on how these elements manifest in digital environments. As a consequence, technology-facilitated trafficking often remains under-identified or mis-



classified within established legal categories, particularly where exploitation is mediated through platforms, anonymised communication or cross-border digital infrastructures.

Conceptually, technology-facilitated trafficking intersects with broader categories of cyber-enabled crime, while remaining distinct in its reliance on coercion, exploitation and sustained control over victims. Unlike standalone cybercrimes, trafficking in human beings involves ongoing relationships between perpetrators and victims, which are increasingly maintained through digital means. This blurring of boundaries complicates classification, investigation and data collection, and contributes to inconsistent responses across jurisdictions.

From a policy perspective, the challenge lies not in the absence of legal instruments, but in the gap between formal recognition and practical implementation. While legal and strategic frameworks acknowledge digital risks, institutional capacities, investigative tools and victim support mechanisms often lag behind the realities of online exploitation. Addressing technology-facilitated trafficking therefore requires not only legal compliance, but also adaptive interpretations, operational guidance and enhanced coordination between criminal justice actors, social services and digital platforms, as well as greater recognition of the intersections between trafficking in human beings and other cyber-enabled forms of criminality that increasingly converge in digital environments.



3. Methodology and Analytical Approach

This article adopts a qualitative, expert-based analytical approach to examine the impact of digitalisation on trafficking in human beings. While it does not constitute a primary empirical study, the analysis is informed by a combination of policy monitoring, review of available qualitative and quantitative data, institutional engagement and extensive professional practice in the fields of anti-trafficking, child protection and digital and online safety. This approach allows for an in-depth examination of emerging trends, operational challenges and institutional responses, including dynamics and patterns that are often underreported or insufficiently captured through quantitative data alone.

The analysis is informed by a review of international and European legal and policy instruments, strategic documents and thematic reports addressing trafficking in human beings, online exploitation and platform governance. Particular attention is paid to instruments and guidance developed within the frameworks of the Council of Europe and the European Union, as well as to evolving regulatory initiatives related to digital services and online child protection.

In addition, the article draws on insights gained through direct engagement with national authorities, law enforcement bodies, judicial actors, victim support services and civil society organisations involved in the prevention of trafficking, victim identification and protection. These insights reflect practical challenges encountered in the detection, investigation and prosecution of technology-facilitated trafficking, as well as in the provision of assistance to victims whose exploitation is mediated or sustained through digital means.

The analytical approach is thematic and problem-oriented, focusing on how digitalisation reshapes the profiles of traffickers and victims, alters trafficking modus operandi, generates and amplifies vulnerabilities to exploitation, and affects institutional capacities across different stages of the anti-trafficking response. While the analysis is primarily qualitative



and illustrative, it aims to identify patterns, cross-cutting dynamics and systemic challenges that are relevant across jurisdictions, rather than to assess individual cases.

Finally, the article acknowledges the limitations inherent in an expert-based qualitative analysis. The findings do not claim to be exhaustive or statistically representative, but instead seek to contribute to ongoing policy and professional debates by highlighting critical gaps, emerging risks and promising practices in addressing technology-facilitated trafficking in human beings.



4. Digitalisation of Trafficking in Human Beings: Challenges in Practice

Digitalisation has fundamentally reshaped how trafficking in human beings is organised, executed and sustained in practice. Across different forms of exploitation, digital technologies increasingly mediate the interaction between traffickers, victims and third parties, influencing recruitment strategies, control mechanisms and profit generation. These changes do not replace traditional forms of trafficking, but rather coexist with and amplify them, creating hybrid models of exploitation that combine online and offline elements, including cases where victims are recruited through social media or online platforms and subsequently exploited in physical settings, as reflected in GRETA's fourth evaluation round³ findings.

From an operational perspective, digitalisation introduces a range of practical challenges for prevention, detection and victim protection. Trafficking activities are increasingly decentralised, fragmented across multiple platforms and jurisdictions, and embedded within legitimate online services, complicating attribution and intervention. At the same time, digital environments reshape risk profiles, vulnerabilities and power asymmetries, affecting both the behaviour of perpetrators and the experiences of victims. The following sub-sections examine these challenges by analysing how digitalisation transforms the profiles of traffickers and victims, alters trafficking modus operandi, and complicates detection, identification and evidentiary processes in practice.

4.1. Digitalisation of the Trafficker's Profile

Digitalisation has significantly altered the profile of traffickers involved in human trafficking, lowering barriers to entry while simultaneously enabling new forms of organisation and control. Whereas trafficking has traditionally been associated with structured criminal networks requiring physical proximity, logistical capacity and direct contact with victims, digital environments increasingly allow perpetrators to operate remote-



ly, anonymously and with reduced visibility. This shift has broadened the spectrum of actors involved in trafficking, ranging from organised criminal groups adapting their operations to online environments to small-scale or individual perpetrators enabled by digital platforms.

In cases of sexual exploitation in particular, social media profiles, messaging applications and platform-based content are used to advertise victims, display images or videos, and signal availability to potential buyers across a range of social media, live-streaming and content-sharing platforms, including those enabling direct interaction and monetisation⁴. These digital “catalogues” allow traffickers to reach a wide audience with minimal cost, rapidly update content, and tailor presentation to different markets, while obscuring the exploitative nature of the underlying activity.

Digitalisation has also reshaped the skill set required to engage in trafficking-related activities. Beyond traditional forms of coercion and control, traffickers increasingly rely on digital competencies, including the ability to navigate social media ecosystems, exploit platform algorithms, manage multiple online identities and use encrypted communication tools. Skills related to online marketing, image curation, audience engagement and financial transactions through digital payment systems have become integral to trafficking operations. In this context, trafficking increasingly intersects with practices commonly associated with influencer culture, online advertising and platform-based commerce.

At the same time, digital environments enable the fragmentation and decentralisation of trafficking operations. Tasks such as recruitment, advertising, communication with buyers, financial management, control and surveillance of victims can be distributed across platforms or delegated to intermediaries, reducing the need for direct involvement and limiting exposure to detection. In some cases, perpetrators operate entirely remotely, coordinating exploitation across borders without physical presence in the country where exploitation occurs, while maintaining control over victims through continuous digital communication, monitoring and coercive online practices. This dispersal of roles complicates the identification



of hierarchical structures and challenges traditional indicators used to assess organised criminal activity.

Digital tools are increasingly used by traffickers to facilitate new and less visible forms of coercion and control over victims. Digital forms of coercion, including threats of exposure, blackmail and the misuse of intimate images or personal data, increasingly replace or complement physical force. At the same time, continuous monitoring through messaging applications, location-sharing functions and the manipulation of online identities enables persistent control over victims' behaviour and movements. Recorded images, videos or personal data are frequently used to reinforce dependency and compliance, particularly in cases involving sexual exploitation and children. These mechanisms are persistent, scalable and difficult to detect, while leaving limited physical evidence.

Finally, the digitalisation of the trafficker's profile contributes to the convergence of trafficking with other forms of online criminality. Perpetrators may operate in overlapping spaces with actors involved in online sexual abuse, fraud or cyber-enabled exploitation, blurring the boundaries between criminal categories. This convergence increases the risk that trafficking-related conduct is misclassified or addressed in isolation, rather than recognised as part of a sustained exploitative relationship.

Overall, the evolution of the trafficker's profile reflects a shift from visibly organised, location-bound structures towards more flexible, digitally skilled and adaptive forms of criminal activity. Understanding these changing profiles and competencies is essential for developing effective prevention, detection and investigative strategies capable of addressing technology-facilitated trafficking in practice.

4.2. Digitalisation of the Victim's Profile

Digitalisation has profoundly affected the profile of victims of trafficking in human beings, reshaping patterns of vulnerability, recruitment and self-identification. Online environments increasingly constitute the first point of contact between traffickers and victims, particularly for children



and young people, but also for adults seeking employment, relationships or opportunities for mobility. As a result, victimisation often begins in seemingly legitimate or familiar digital spaces, blurring the boundaries between voluntary online engagement and exploitative outcomes.

Digital platforms facilitate targeted recruitment by enabling traffickers to identify and approach individuals based on age, gender, location, socioeconomic background, migration status or expressed interests. Social media profiles, online communities and messaging applications provide access to extensive personal information, much of which is voluntarily shared by users without awareness of its potential long-term implications. Perceived anonymity and a sense of safety in online environments can lower individual caution, leading users to disclose personal details, images, preferences and vulnerabilities that contribute to the construction of a visible online persona. This self-generated digital footprint shapes how individuals are perceived by others and can inadvertently increase their attractiveness to perpetrators seeking to identify and approach potential victims. Traffickers use this information to tailor their recruitment strategies, build trust and gradually draw victims into dependent and exploitative relationships. This process often involves the use of manipulative techniques, including emotional influence, the creation of a perceived sense of closeness and trust, as well as the involvement of victims in the creation or sharing of intimate content, which may subsequently be used for blackmail and control. In this context, grooming processes may develop over extended periods of time and across multiple platforms, making them particularly difficult to detect and disrupt.

The digitalisation of recruitment has also contributed to changes in victims' self-perception and pathways into exploitation. In some cases, individuals may initially perceive their involvement as consensual, opportunistic or temporary, particularly where exploitation is framed as work, self-employment or online activity. This is especially evident in cases of sexual exploitation mediated through digital platforms, where the line between content creation, commercial sex and trafficking can appear



blurred. Such dynamics can delay, distort or even prevent self-identification as a victim, thereby reducing the likelihood of seeking assistance or engaging with support services.

Digital environments create specific conditions in which victims develop forms of dependency and subordination that are less visible, yet equally powerful and coercive. Continuous online communication, the possibility of constant monitoring, and the threat of dissemination of intimate images, videos or personal data reinforce feelings of fear, shame and isolation. For many victims, particularly children and young people, the experience of exploitation is often accompanied by confusion, feelings of guilt and the gradual normalisation of the situation, which further hinders its recognition as abuse. In this context, victims often do not self-identify as such, experience strong concerns about disclosure, and face significant internal barriers to seeking assistance or resisting the perpetrator.

Digitalisation has also affected the visibility and identification of victims by authorities and support services. Victims whose exploitation is primarily mediated online may have limited physical contact with perpetrators, may not be confined to specific locations, may not display traditional indicators of trafficking, and may not even know with certainty the identity of those exploiting them. This challenges established identification practices and increases the risk that victims remain undetected or are misclassified, particularly where exploitation intersects with other forms of online abuse or irregular economic activity.

Overall, the digitalisation of the victim's profile reflects a shift towards less visible, more fragmented and often internally normalised forms of exploitation. Understanding how digital environments shape vulnerability, agency and control is essential for developing effective prevention, identification and support measures that respond to the lived realities of victims in technology-facilitated trafficking cases.



4.3. Modus Operandi in Technology-Facilitated Trafficking

Digitalisation has transformed the modus operandi of trafficking in human beings by embedding exploitative practices within ordinary online activities and services. Rather than relying solely on physical movement or confinement, technology-facilitated trafficking often unfolds through a sequence of digitally mediated actions spanning multiple platforms, jurisdictions and stages of exploitation. GRETA has observed that information and communication technologies (ICT) are used across the trafficking process—particularly for recruiting and controlling victims—while also noting that the evidence base has historically been fragmented and uneven across States.

Recruitment increasingly begins in online environments, including social media, messaging applications, dating apps, and online job advertisements. GRETA's monitoring and research highlight that recruitment via social media and dating applications is a recurrent pattern, and that ICT can facilitate the identification, location and contact of potential victims. Europol similarly notes that trafficking has evolved into a “business model” in which the online component forms an essential part of offenders' modus operandi, enabling them to operate behind a “virtual shield” while still generating exploitable digital traces. Over time, traffickers commonly move interactions from public or semi-public spaces to private or encrypted channels, which complicates early detection and limits the effectiveness of isolated interventions.

Exploitation itself is increasingly mediated through digital tools. In cases of sexual exploitation, victims may be compelled to produce images, videos or live-streamed content, while traffickers control distribution, “advertising,” pricing and interaction with buyers. GRETA has documented that ICT is used not only for recruitment but also for exerting control and pressure over victims, including maintaining contact even after victims leave exploitation in order to intimidate them and deter reporting. Technology also shapes labour exploitation dynamics through digital coordination, remote supervision and platform-enabled intermediation, particularly in



informal or precarious labour settings—changes which ICAT describes as part of broader technology-driven shifts affecting trafficking trends, challenges and opportunities.

Control mechanisms in technology-facilitated trafficking often rely less on physical restraint and more on psychological pressure, surveillance and digital dependency. Continuous connectivity enables real-time monitoring through messaging applications, location-sharing features and persistent digital contact. Threats related to the dissemination of intimate images or personal data can operate as a form of coercive leverage, intensifying fear and compliance—dynamics that align with GRETA's analysis of ICT-facilitated control strategies.

Digitalisation has also reshaped trafficking for the purpose of forced criminality, an area increasingly highlighted by both law enforcement and monitoring bodies. Findings from Europol and GRETA indicate that children and vulnerable adults are increasingly recruited online for activities such as forced theft, involvement in drug distribution, benefit fraud, online scams and other forms of criminal exploitation, often facilitated through social media, messaging applications or gaming platforms. Digital tools facilitate remote instruction, supervision and control, allowing traffickers to direct criminal activities while minimising direct contact and exposure. GRETA has noted that digital communication is used to maintain constant control over victims, issue instructions, monitor performance and enforce compliance through threats, debt manipulation or the misuse of personal data. ICAT further highlights that technology enables the rapid adaptation and scaling of trafficking for criminal exploitation, while contributing to the misidentification of victims as offenders. These digitally mediated dynamics complicate detection and victim identification, as individuals exploited for criminality are frequently treated primarily as perpetrators, reinforcing under-identification and limiting access to protection and assistance.

Digitalisation has further blurred the boundaries between the sexual exploitation of children, the growing availability of child sexual abuse material (CSAM), and trafficking in children for the purpose of sexual ex-



ploitation. Europol has consistently reported a significant increase in online CSAM, including material that is self-produced by children under conditions of coercion, manipulation or grooming. While such material is often treated primarily within a child sexual abuse framework, GRETA has emphasised that these dynamics frequently intersect with trafficking, particularly where the production, distribution or monetisation of images and videos is organised or controlled by third parties. In technology-facilitated trafficking cases, self-generated sexual content may constitute an entry point into sustained exploitation, with images or videos subsequently used to exert control, blackmail victims or enable repeated abuse by multiple perpetrators. These overlapping dynamics challenge traditional legal and operational distinctions between CSAM-related offences and trafficking in human beings, increasing the risk of fragmented responses, misclassification of cases and insufficient recognition of child victims' trafficking-specific protection needs.

Financial flows associated with trafficking are also affected by digitalisation. Europol highlights that core elements of criminal processes are increasingly moving online, including payment systems, and that digitalisation supports speed, reach and concealment across serious and organised crime more broadly. In trafficking contexts, this translates into greater use of online transactions, platform-mediated payments, and cross-border fragmentation of financial trails, raising practical barriers for financial investigations and asset recovery.

Overall, the modus operandi of technology-facilitated trafficking reflects a shift towards more decentralised, adaptive and resilient forms of exploitation. GRETA emphasises the need for law enforcement and criminal justice systems to adapt to these structural changes in how people interact and how trafficking is carried out, while Europol underlines the growing centrality of online components in trafficking operations. Understanding these evolving operational patterns is essential for developing effective investigative strategies, disrupting exploitative networks and ensuring timely



identification and protection of victims in practice. Recent findings from the Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children, further highlight the increasing involvement of children in criminal exploitation and the role of online environments in recruitment and control.

The increasing overlap between trafficking in human beings, child sexual exploitation and CSAM-related offences raises broader questions about the adequacy of existing legal and operational approaches to crime classification and investigation in digitally mediated cases. While these crimes are governed by distinct legal frameworks, digitalisation has eroded traditional boundaries between them, creating situations in which a single case may simultaneously involve elements of trafficking, online sexual abuse and the production or distribution of CSAM. In practice, this blurring of categories often results in investigative strategies that prioritise the offence perceived as easier to prove or more likely to result in successful prosecution, rather than reflecting the full scope of exploitation involved. This raises critical questions as to whether current responses require further development of legal frameworks, or whether greater emphasis should be placed on flexible, victim-centred and operationally integrated investigations that allow multiple offences to be examined in parallel. Moving beyond investigative approaches that require choosing a single offence, and towards recognising that multiple forms of exploitation may coexist within the same case, may be essential for ensuring accountability, avoiding fragmented proceedings and securing comprehensive protection for victims.

4.4. Detection, Identification and Evidentiary Challenges

The digitalisation of trafficking in human beings has introduced significant challenges for detection, identification and evidence-gathering, exposing limitations in traditional investigative approaches that rely on physical indicators, territorial presence and linear crime narratives. Technology-facilitated trafficking is often decentralised, transnational and



embedded within legitimate online environments, making it difficult for authorities to identify cases at an early stage and to establish clear links between perpetrators, victims and exploitative conduct.

One of the primary challenges lies in victim identification. Victims whose exploitation is mediated through digital platforms may not be physically confined, may have limited direct contact with traffickers and may not self-identify as victims, particularly where exploitation is framed as voluntary online activity or informal work. As highlighted by GRETA, technology-facilitated trafficking cases are frequently under-identified, with victims remaining invisible to authorities or misclassified under other forms of abuse or criminal activity. This risk is particularly acute for children and for victims exploited for forced criminality, who may be treated primarily as offenders rather than as victims of trafficking.

Detection is further complicated by the fragmented and platform-dependent nature of digital evidence. Trafficking-related activities may be distributed across multiple online services, including social media platforms, messaging applications, payment systems and cloud storage, often located in different jurisdictions. Europol has repeatedly underlined that while digitalisation leaves exploitable data traces, accessing, preserving and correlating this information remains operationally complex. Delays in data preservation, challenges in cross-border cooperation and inconsistencies in platform responsiveness can critically undermine investigations.

Evidentiary challenges are also closely linked to the classification of offences. Where cases involve overlapping elements of trafficking, sexual exploitation, CSAM-related offences or forced criminality, investigative strategies may prioritise the offence perceived as easier to prove or more likely to lead to conviction. While such decisions may be driven by practical constraints, they risk narrowing the evidentiary scope, fragmenting cases and obscuring the sustained and exploitative nature of the conduct. GRETA has noted that technology-facilitated trafficking often remains insufficiently reflected in prosecutions, partly due to difficulties in meeting evidentiary thresholds for trafficking-specific offences in digital contexts.



The assessment of coercion, control and exploitation presents additional challenges in online settings. Digital forms of control—such as constant communication, surveillance, threats of exposure or the misuse of intimate images—may be less visible than physical violence but are no less effective. However, these forms of coercion are not always readily recognised within existing evidentiary frameworks, particularly where legal interpretations continue to privilege physical indicators of force or confinement. This can result in the underestimation of harm and the mischaracterisation of exploitative relationships.

Finally, institutional capacity and expertise play a decisive role. Effective detection and investigation of technology-facilitated trafficking require specialised skills in digital forensics, online investigation and platform engagement, as well as sustained cooperation between law enforcement, prosecutors, victim support services and technology companies. Both GRETA and Europol have stressed that gaps in training, resources and inter-agency coordination continue to limit the ability of authorities to respond effectively to digitally mediated forms of trafficking.

Taken together, these challenges demonstrate that digitalisation does not merely add complexity to existing trafficking cases, but fundamentally reshapes the conditions under which exploitation is detected, investigated and prosecuted. Addressing these challenges requires adaptive investigative practices, flexible legal interpretations and integrated responses capable of capturing the full scope of exploitation in technology-facilitated trafficking cases.



5. Impact of Digitalisation on Victims

Digitalisation has significantly transformed the experiences of victims of trafficking in human beings, shaping both their pathways into exploitation and their ability to seek help and exit abusive situations. Online environments expand the reach of traffickers and increase exposure to risk, particularly for children and young people, while simultaneously altering how victims perceive, experience and respond to exploitation.

The integration of digital technologies into everyday life has created new spaces in which vulnerabilities can emerge and be exploited, often in ways that are less visible and more difficult to recognise. Recruitment, manipulation and control can occur remotely, gradually and across multiple platforms, reducing the likelihood that victims or those around them identify the situation as exploitation at an early stage. As a result, the boundaries between voluntary interaction, risky behaviour and coercion may become increasingly blurred.

At the same time, digitalisation enables exploitation to be more persistent, scalable and intrusive. Victims may be subjected to continuous monitoring, repeated exposure and the ongoing circulation of exploitative content, which can extend harm beyond the immediate situation of exploitation. These dynamics not only intensify the impact on victims but also complicate their ability to disengage, seek assistance and rebuild autonomy.

5.1. Online vulnerabilities and exploitation dynamics

Digitalisation has significantly transformed the experiences of victims of trafficking in human beings, shaping both their pathways into exploitation and their ability to seek help and exit abusive situations. Online environments expand the reach of traffickers and increase exposure to risk, particularly for children and young people, while simultaneously altering how victims perceive, experience and respond to exploitation.

The integration of digital technologies into everyday life has created new spaces in which vulnerabilities can emerge and be exploited, often in ways



that are less visible and more difficult to recognise. Recruitment, manipulation and control can occur remotely, gradually and across multiple platforms, reducing the likelihood that victims or those around them identify the situation as exploitation at an early stage. As a result, the boundaries between voluntary interaction, risky behaviour and coercion may become increasingly blurred.

At the same time, digitalisation enables exploitation to be more persistent, scalable and intrusive. Victims may be subjected to continuous monitoring, repeated exposure and the ongoing circulation of exploitative content, which can extend harm beyond the immediate situation of exploitation. These dynamics not only intensify the impact on victims but also complicate their ability to disengage, seek assistance and rebuild autonomy.

In addition, digital environments can contribute to forms of psychological control and dependency that are less visible than physical coercion but equally powerful. The use of manipulation, emotional pressure, threats of exposure and the exploitation of personal data can create sustained fear and compliance, even in the absence of direct physical restraint. In such contexts, victims may experience confusion, self-blame or a diminished perception of harm, further delaying recognition of exploitation and access to support.

Digitalisation also affects the social context in which exploitation occurs. Victims may remain physically embedded within their communities, families or peer networks while being simultaneously exploited online, making the situation harder for others to detect. This “hidden in plain sight” dynamic reduces opportunities for external intervention and reinforces isolation, particularly where victims maintain an outward appearance of normality.

Taken together, these developments highlight the need to understand victim experiences in technology-facilitated trafficking as complex, dynamic and often non-linear, requiring responses that go beyond traditional indicators and address the specific risks and harms associated with digital



environments. Strengthening digital media literacy and resilience among children, young people and other vulnerable groups is an essential component of such responses, enabling individuals to better recognise risks, critically assess online interactions and seek support when needed. Preventive approaches that combine awareness, skills-building and accessible support mechanisms can play a key role in reducing vulnerability to online recruitment and exploitation.

5.2. Risks of secondary victimisation and barriers to protection

Digitalisation also introduces new risks of secondary victimisation and creates additional barriers to identification and protection. The permanence and potential uncontrolled dissemination of online content, including images and videos, can generate lasting fear, shame and psychological harm, discouraging victims from seeking assistance or cooperating with authorities. In many cases, victims may fear that reporting exploitation will lead to further exposure or continued circulation of harmful material, reinforcing silence and non-disclosure.

At the same time, victims whose exploitation is primarily mediated online may not display traditional indicators of trafficking. They may not be physically confined, may have limited or no direct contact with perpetrators, and may not even know with certainty the identity of those exploiting them. These factors complicate identification and increase the risk that victims are overlooked or misclassified within criminal justice systems.

Digitalisation also affects the nature of evidence and its use in proceedings, which may inadvertently contribute to secondary victimisation. Victims may be repeatedly exposed to exploitative material during investigations and court proceedings, while the use of digital evidence—such as images, videos or communication records—can prolong trauma and reinforce feelings of loss of control. In addition, cross-border elements of digital cases may lead to delays, fragmented procedures or limited access to information, further weakening trust in authorities and support systems.



Furthermore, victims involved in criminal activities as a result of exploitation—particularly children—may be treated as offenders rather than victims, reinforcing barriers to protection. This is particularly relevant in cases of forced criminality, including online-enabled offences, where the link between exploitation and criminal conduct may not be immediately recognised. As a result, victims may face prosecution, detention or administrative sanctions instead of receiving protection and assistance.

Addressing these challenges requires a shift towards more flexible, victim-centred identification approaches that recognise the complex and often non-linear nature of technology-facilitated exploitation. It also requires safeguards to prevent secondary victimisation throughout investigative and judicial processes, including careful handling of digital evidence, trauma-informed procedures and strengthened coordination between criminal justice and victim support actors.



6. Global Trends and Emerging Patterns

The digitalisation of trafficking in human beings reflects broader global trends in the evolution of organised crime, where technology enables greater scale, speed and adaptability. Trafficking networks increasingly operate across digital and physical environments, creating hybrid and transnational models of exploitation that challenge traditional forms of detection and response. These developments are not isolated, but form part of a wider shift towards more decentralised, networked and technology-enabled forms of criminal activity.

At a global level, digitalisation has contributed to the diversification of trafficking patterns, enabling perpetrators to target a wider pool of victims, operate across multiple markets simultaneously and rapidly adapt their methods in response to law enforcement interventions. The convergence between trafficking and other forms of organised crime, including cyber-enabled offences, financial crime and online sexual exploitation, is becoming increasingly evident, further complicating classification and response.

6.1. Cross-border and platform-based exploitation

Technology-facilitated trafficking is inherently transnational. Online platforms allow perpetrators to recruit, control and exploit victims across multiple jurisdictions simultaneously, often without physical presence in the country where exploitation occurs. This creates significant challenges for law enforcement and judicial authorities, particularly in relation to jurisdiction, evidence-gathering and cross-border cooperation.

At the same time, digital infrastructures enable perpetrators to operate through distributed networks rather than hierarchical structures, with different actors performing specialised roles across countries and platforms. This fragmentation complicates the identification of organised criminal groups and challenges traditional investigative approaches that rely on clear organisational structures. In addition, perpetrators increas-



ingly use private or closed online groups, including time-limited or invitation-based communication channels, to coordinate activities and evade detection, sometimes exploiting periods of reduced monitoring or enforcement capacity, such as weekends or outside standard working hours.

Platform-based ecosystems also enable the rapid dissemination of exploitative content and the coordination of criminal activities at scale. The use of social media, messaging applications, online marketplaces and encrypted communication channels facilitates the fragmentation of trafficking operations, while simultaneously connecting actors, victims and buyers in complex digital networks. In some cases, platforms function as intermediaries that facilitate contact, negotiation and exploitation, blurring the boundaries between legal and illegal activities.

In addition, cross-border digital environments can create gaps in protection, as victims may be recruited in one country, exploited in another and controlled from a third jurisdiction. These dynamics complicate access to assistance, delay identification and may result in fragmented or inconsistent responses across jurisdictions.

6.2. Technology outpacing regulatory and institutional responses

A key emerging pattern is the growing gap between the pace of technological development and the ability of regulatory and institutional frameworks to respond effectively. While legal instruments increasingly acknowledge the role of digital technologies in trafficking, operational capacities, investigative tools and cross-border cooperation mechanisms often lag behind.

Emerging technologies, including artificial intelligence, anonymisation tools and encrypted communication systems, continue to reshape the landscape of exploitation, creating new opportunities for perpetrators while complicating detection and prosecution. At the same time, traf-



fickers demonstrate a high level of adaptability, quickly shifting between platforms, tools and methods in response to regulatory measures and enforcement actions.

Another challenge lies in the fragmentation of legal and regulatory approaches across jurisdictions. Differences in legislation, data protection regimes and procedural rules can hinder timely access to digital evidence and limit effective cooperation between authorities. In addition, the involvement of private-sector actors, particularly digital platforms, introduces further complexity in terms of responsibilities, accountability and access to data.

Limited data availability and inconsistencies in classification further hinder a comprehensive understanding of technology-facilitated trafficking. Many cases remain under-identified or are recorded under different offence categories, making it difficult to capture the scale and nature of the phenomenon. As a result, policy responses are often based on incomplete or fragmented information.

Addressing these challenges requires continuous adaptation, investment in expertise and stronger integration between legal, technological and policy responses at both national and international levels. It also requires enhanced data collection, improved analytical capacities and sustained exchange of practices to ensure that responses remain effective in a rapidly evolving digital environment.



7. Good Practices and Emerging Responses

7.1. Inter-institutional and Multi-stakeholder Approaches

Addressing technology-facilitated trafficking in human beings increasingly requires coordinated responses that extend beyond traditional law enforcement action. Good practices emerging across Europe highlight the importance of structured cooperation between law enforcement authorities, prosecutors, child protection services, victim support organisations, regulators and technology companies. Such cooperation is essential to capture the full scope of digitally mediated exploitation, particularly in cases involving overlapping offences such as trafficking, online sexual abuse and forced criminality.

Monitoring findings of GRETA emphasise that effective responses depend on early information-sharing and joint analysis across sectors. Multidisciplinary teams combining investigative, prosecutorial and victim-support expertise have proven particularly valuable in complex cases where digital evidence, victim identification and protection must be addressed simultaneously. These approaches help avoid fragmented case handling and reduce the risk that victims are misidentified or excluded from assistance due to narrow crime classification.

Emerging practices also point to the growing role of cooperation with technology companies and platform providers. While challenges persist regarding data access, response times and jurisdictional constraints, structured engagement mechanisms—such as designated law enforcement contact points, trusted flagger systems⁵ and platform-specific reporting channels—have improved the ability of authorities to identify and preserve relevant digital evidence. Europol has highlighted that proactive collaboration with private-sector actors is increasingly essential for disrupting trafficking operations that rely heavily on online services and digital infrastructure.

Capacity-building remains a critical component of effective inter-institu-



tional responses. Good practices include specialised training for investigators, prosecutors and judges on technology-facilitated trafficking, digital forms of coercion and the use of online evidence. Equally important is the inclusion of victim-centred perspectives in operational responses, ensuring that investigative strategies do not exacerbate harm or reinforce barriers to disclosure and protection.

Given the inherently transnational nature of technology-facilitated trafficking, international cooperation is a critical component of effective responses. Digital environments enable perpetrators to operate across multiple jurisdictions simultaneously, making timely cross-border information exchange, joint investigations and coordinated action essential. Existing mechanisms, including Europol-supported cooperation, mutual legal assistance and joint investigation teams, play a key role, but challenges remain in relation to data access, differing legal frameworks and procedural delays. Strengthening international cooperation, including with countries outside the European Union, is therefore essential to ensure effective investigation, prosecution and victim protection in digitally mediated trafficking cases.

7.2. Reporting Mechanisms and Specialised Responses

Effective reporting and referral mechanisms are central to the early detection of technology-facilitated trafficking, particularly in cases involving children and online exploitation. Good practices increasingly emphasise the need for accessible, well-publicised reporting channels that allow victims, professionals and third parties to flag suspected exploitation in digital environments. This includes online reporting tools⁶, hotlines and platform-based reporting functions designed to capture trafficking-related indicators alongside other forms of online abuse.

Specialised responses have proven particularly important where exploitation occurs primarily online or across borders. Dedicated units within law enforcement agencies, specialised prosecutors and child protection services with digital expertise are better positioned to assess complex cases



involving multiple platforms and overlapping offences. GRETA has noted that the absence of such specialised structures often leads to delays, misclassification and missed opportunities for victim protection, especially in technology-facilitated cases.⁷

Promising practices also include the integration of reporting mechanisms into broader victim referral systems. Ensuring that reports related to on-line exploitation trigger both investigative action and protective measures helps bridge the gap between detection and assistance. In child trafficking cases, close coordination between law enforcement, child protection authorities and specialised NGOs is essential to ensure that children are recognised as victims of trafficking and provided with appropriate support, regardless of how exploitation initially comes to light.

Finally, emerging responses highlight the importance of adaptability. As digital platforms, communication tools and exploitation patterns evolve rapidly, reporting mechanisms and institutional responses must be regularly reviewed and updated. Flexible procedures, continuous training and sustained dialogue between stakeholders are key to ensuring that good practices remain effective in an increasingly digitalised environment.

7.3. Prevention-Oriented and Resilience-Building Approaches

Preventing technology-facilitated trafficking in human beings requires sustained investment in building resilience among children, young people and other vulnerable groups in digital environments. Good practices increasingly emphasise prevention strategies that address online risks, power imbalances and exploitative dynamics before harm occurs. This includes initiatives aimed at strengthening digital literacy, critical thinking and awareness of online grooming and manipulation, as well as promoting safer online behaviour without placing responsibility on potential victims.

Models such as national Safer Internet Centres and dedicated hotlines provide valuable examples of integrated prevention frameworks. Through education, awareness-raising, counselling and reporting mechanisms,



these structures contribute to early identification of risks and to the disruption of harmful online content and behaviour. Their close cooperation with schools, civil society organisations, law enforcement authorities and technology companies enables a comprehensive approach to online safety that is particularly relevant in the context of child trafficking and online sexual exploitation.

Targeted prevention measures are also essential for adults and groups facing heightened vulnerability, including migrants, children in alternative care, young people transitioning out of institutional settings and individuals experiencing socioeconomic exclusion. Tailored outreach, community-based interventions and culturally sensitive information campaigns have shown promise in reducing exposure to online recruitment and exploitation, particularly when combined with accessible support services.

Public-private partnerships play an increasingly important role in prevention efforts. Cooperation between public authorities, civil society and digital service providers can enhance risk assessment, content moderation, reporting pathways and the dissemination of preventive information. The involvement of technology companies in identifying systemic risks, supporting awareness campaigns and facilitating user reporting contributes to a more proactive prevention ecosystem, while underscoring the shared responsibility for addressing online-facilitated exploitation.

Overall, prevention-oriented approaches complement investigative and protective responses by addressing the underlying conditions that enable technology-facilitated trafficking. Strengthening resilience, promoting informed online engagement and fostering coordinated prevention strategies are critical components of a comprehensive response to trafficking in an increasingly digitalised environment.

Emerging responses are also increasingly exploring the use of artificial intelligence (AI) and automated tools to support the detection and prevention of technology-facilitated trafficking in human beings. AI-based systems are already used by digital platforms to identify patterns associ-



ated with child sexual abuse material, coordinated exploitation networks and suspicious user behaviour at scale. Digital forensic tools, commonly used in CSAM investigations, are now also applied in cases of trafficking in human beings to analyse online communications, recover and preserve digital evidence and support the identification of victims and perpetrators.

In trafficking-related contexts, such tools have the potential to support early risk detection, identify recruitment patterns, flag repeated exploitation indicators and enhance the prioritisation of reports. In addition, some countries, including the Netherlands, Germany, Norway and the United Kingdom, use web crawlers and other automated detection tools to identify trafficking-related content online, including advertisements linked to sexual exploitation, thereby supporting proactive investigations and victim identification.

However, their effectiveness depends on transparency, appropriate training data and close human oversight. Without adequate safeguards, AI systems risk reinforcing biases, overlooking less visible forms of exploitation or generating false positives that may harm victims. As a result, good practice points towards the use of AI as a complementary tool within broader investigative, preventive and victim-centred frameworks, rather than as a standalone solution.



8. Policy Implications and Recommendations

The digitalisation of trafficking in human beings has profound implications for policy, legislation and practice. While existing legal frameworks provide a solid normative basis for addressing trafficking, the analysis in this article demonstrates that technology-facilitated exploitation increasingly challenges traditional assumptions about crime classification, victim identification, evidence-gathering and institutional response. Addressing these challenges requires not only legal compliance, but adaptive, coordinated and victim-centred approaches capable of responding to evolving digital realities.

First, policy responses should prioritise flexibility in investigation and prosecution. Where facts indicate the coexistence of multiple forms of exploitation - such as trafficking, child sexual exploitation, CSAM-related offences or forced criminality - authorities should be supported in pursuing parallel or combined investigative strategies, rather than limiting cases to a single legal qualification for reasons of procedural convenience. This requires clear operational guidance, prosecutorial coordination and judicial awareness of digitally mediated forms of coercion and control.

Second, strengthening institutional capacity remains critical. Law enforcement authorities, prosecutors and judges require specialised training on technology-facilitated trafficking, including digital recruitment patterns, online control mechanisms and evidentiary challenges specific to digital environments. Investment in digital forensic expertise, cross-border cooperation mechanisms and timely access to platform-held data is essential to ensure effective investigation and prosecution.

Third, victim identification and protection mechanisms must be adapted to reflect the realities of online exploitation. Identification criteria and referral procedures should explicitly recognise technology-facilitated forms of trafficking, including cases where victims may not self-identify, lack physical indicators of abuse or are initially treated as offenders. In particular, children exploited online and victims of forced criminality require safeguards to prevent criminalisation and ensure access to specialised support services.

Fourth, prevention should be recognised as a core component of responses



to technology-facilitated trafficking. Building resilience among children, young people and other vulnerable groups through digital literacy, awareness-raising and targeted outreach can reduce exposure to online recruitment and exploitation. Integrated models combining education, counselling, reporting mechanisms and public–private cooperation—such as Safer Internet Centres⁸ and hotlines - offer valuable frameworks for early intervention and risk mitigation.

Fifth, cooperation with digital service providers should be strengthened through clear expectations, structured engagement and shared responsibility. Platforms play a central role in shaping online environments and can contribute to risk assessment, reporting pathways and the detection of exploitative patterns. The use of artificial intelligence and automated tools may support these efforts, provided such technologies are deployed transparently, with appropriate safeguards, human oversight and respect for fundamental rights.

Sixth, policy responses should explicitly address the role of digitalisation in generating and amplifying vulnerabilities to trafficking and exploitation. This includes recognising how online environments shape exposure to risk, influence behaviour and enable new forms of targeting, particularly for children and other vulnerable groups. At the same time, the transnational nature of technology-facilitated trafficking requires strengthened international cooperation, including timely cross-border data access, joint investigations and coordination with actors operating across jurisdictions. Enhancing data collection, research and evidence on technology-facilitated trafficking is also essential to better understand evolving patterns of exploitation and to inform effective policy and operational responses.

Finally, policy development should be informed by continuous monitoring, research and exchange of practice at national and international levels. As digital technologies evolve rapidly, responses to trafficking must remain dynamic, evidence-informed and inclusive of multidisciplinary perspectives. Bridging the gap between legal recognition and operational reality is essential to ensuring that responses to technology-facilitated trafficking are effective, proportionate and centred on the rights and needs of victims.



9. Conclusion

Digitalisation has fundamentally reshaped the landscape of trafficking in human beings, transforming how exploitation is initiated, sustained and concealed across borders and platforms. As this article has shown, technology does not create new forms of trafficking, but it profoundly alters the profiles of traffickers and victims, the modus operandi of exploitation, and the conditions under which crimes are detected, investigated and prosecuted. At the same time, it increases vulnerabilities to human trafficking and exploitation across a much larger scale of affected individuals. These transformations challenge traditional assumptions embedded in legal frameworks, institutional practices and evidentiary standards.

The increasing overlap between trafficking, child sexual exploitation, CSAM-related offences and forced criminality exposes the limitations of fragmented legal and operational responses. In digitally mediated contexts, rigid crime classification and fragmented investigative approaches risk obscuring the full scope of exploitation and undermining victim protection. Recognising and addressing the coexistence of multiple forms of exploitation within a single case is therefore essential for effective accountability and comprehensive responses.

At the same time, digitalisation creates opportunities to strengthen prevention, detection and cooperation. Emerging practices demonstrate the value of multidisciplinary approaches, engagement with digital service providers, resilience-building among vulnerable groups and the responsible use of technological tools, including artificial intelligence. However, these opportunities require sustained investment in institutional capacity, operational guidance and safeguards to ensure that responses remain effective and rights-based.

Ultimately, addressing technology-facilitated trafficking requires bridging the gap between legal frameworks and operational realities. As digital environments continue to evolve, responses must remain adaptive,



coordinated and grounded in the protection of victims' rights. Ensuring that systems can respond effectively to these transformations is not only a matter of efficiency, but a prerequisite for meaningful protection in an increasingly digitalised world.

1 **The Dark Web** refers to a small, intentionally hidden part of the internet that is not accessible through standard search engines and requires the use of specialised software, such as Tor, to be accessed. It provides a high level of anonymity for both users and website operators, making it an environment used for both legitimate purposes and illicit activities, including the distribution of illegal content, online marketplaces and communication between offenders.

2 See, inter alia, Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, 2007); Directive 2011/93/EU; Regulation (EU) 2022/2065 (Digital Services Act); and Proposal COM(2022) 209 final.

3 See Council of Europe, Group of Experts on Action against Trafficking in Human Beings (GRETA), 4th Evaluation Round (thematic focus on the impact of information and communication technologies on trafficking in human beings), and GRETA, 11th General Report on GRETA's activities (2022).

4 Examples of such platforms may include widely used social media, live-streaming and subscription-based content services (e.g. OmeTV, OnlyFans, TikTok, Instagram.), which offer functionalities such as direct interaction, content sharing and monetisation and may be misused by perpetrators for exploitative purposes.

5 Under Regulation (EU) 2022/2065 (Digital Services Act), trusted flaggers are entities designated by national Digital Services Coordinators based on their proven expertise and competence in identifying illegal content. Online platforms are required to treat notices submitted by trusted flaggers with priority and without undue delay, thereby enhancing the detection and removal of illegal content and improving the effectiveness of reporting mechanisms.

6 Hotlines operating within the INHOPE network (International Association of Internet Hotlines), which brings together 57 hotlines across more than 50 countries worldwide, provide mechanisms for the public to report illegal online content, including child sexual abuse material. Reports are assessed by trained analysts and, where appropriate, forwarded to law enforcement authorities and online service providers, facilitating content removal, cross-border cooperation and the identification of victims.

7 See GRETA, Fourth Evaluation Round Reports on trafficking in human beings (various countries), Council of Europe, 2021–2025, in particular sections on victim identification, specialised structures and capacity gaps. See also GRETA, 11th General Report on GRETA's Activities (2021), thematic chapter on technology-facilitated trafficking.

8. Network of Safer Internet Centers, <https://better-internet-for-kids.europa.eu/en/sic>.



Bibliography

- 1) Council of Europe. (2005). Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197). <https://rm.coe.int/t/168008371d>
- 2) Council of Europe. (2007). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201). <https://rm.coe.int/1680084822>
- 3) European Parliament and Council of the European Union. (2011a). Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0036>
- 4) European Parliament and Council of the European Union. (2024). Directive (EU) 2024/1712 amending Directive 2011/36/EU. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1712>
- 5) European Parliament and Council of the European Union. (2011b). Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093>
- 6) European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065>
- 7) European Commission. (2022). Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209>
- 8) Council of Europe, GRETA. (2022). 11th General Report on GRETA's activities. <https://rm.coe.int/greta-11th-general-report-of-activities-2022-en/1680a72bb8>
- 9) Council of Europe, GRETA. (2021). 10th General Report on GRETA's activities. <https://rm.coe.int/10th-general-report-on-greta-activities/1680a2d43b>
- 10) Council of Europe. (2020). Online and technology-facilitated trafficking in human beings (GRETA thematic chapter in General Report). <https://www.coe.int/en/web/anti-human-trafficking/online-and-technology-facilitated-trafficking-in-human-beings>
- 11) UNODC. (2022). Global Report on Trafficking in Persons. <https://www.unodc.org/unodc/en/data-and-analysis/glotip.html>



- 12) Inter-Agency Coordination Group against Trafficking in Persons (ICAT). (2023). Issue brief: The role of technology in trafficking in persons. <https://icat.un.org/publications>
- 13) ICAT, 2020, Technology and Trafficking in Persons during COVID-19 and beyond, <https://icat.un.org/events/05-2020/technology-and-trafficking-persons-during-covid-19-and-beyond>
- 14) ICAT, 2019, Issue Brief 7, Human Trafficking and Technology: trends, challenges and opportunities, https://icat.un.org/sites/g/files/tmzbd461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf
- 15) ICAT, 2022, Use and abuse of technology, https://icat.un.org/sites/g/files/tmzbd461/files/publications/icat_statement_wdat_2022.pdf
- 16) ICAT, 2022, Issue Brief 12, Addressing vulnerabilities to Trafficking in Persons, https://icat.un.org/sites/g/files/tmzbd461/files/publications/icat_issue_brief_12_vulnerability_to_tip.pdf
- 17) Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment>
- 18) Europol. (2025). European Union Serious and Organised Crime Threat Assessment (EU SOCTA). <https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment>
- 19) WeProtect Global Alliance. (2021). Global Threat Assessment 2021. <https://www.weprotect.org/global-threat-assessment-21/>
- 20) Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children. (2024). Annual figures Human Trafficking 2023. <https://www.dutchrapporteur.nl/documents/2024/10/18/annual-figures-human-trafficking-2023>
- 21) Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children. (2024). Broad perspectives of offending: backgrounds of domestic sex traffickers. <https://www.dutchrapporteur.nl/documents/2025/04/04/broad-perspective-on-offending-backgrounds-of-domestic-sex-traffickers>
- 22) OSCE. (2024). Policy action to address technology-facilitated trafficking in human beings. <https://cthb.osce.org/cthb/579190>
- 23) Aronowitz, A. A. (2009). Human trafficking, human misery: The global trade in human beings. Praeger, https://www.researchgate.net/publication/373884084_Human_Trafficking_Human_Misery_The_Global_Trade_in_



Human Beings

- 24) Shelley, L. (2010). Human trafficking: A global perspective. Cambridge University Press. https://assets.cambridge.org/9780521113816/excerpt/9780521113816_excerpt.pdf
- 25) Lee, M. (Ed.). (2011). Trafficking and global crime control. Sage. https://sk.sagepub.com/book/mono/trafficking-and-global-crime-control/toc#_
- 26) Kempadoo, K., Sanghera, J., & Pattanaik, B. (Eds.). (2015). Trafficking and prostitution reconsidered. Routledge. https://christusliberat.org/journal/wp-content/uploads/2018/08/Trafficking-and-Prostitution-Reconsidered_-Kamala-Kempadoo.pdf
- 27) Broad, R., & Turnbull, N. (2019). From human trafficking to modern slavery. *European Journal on Criminal Policy and Research*, 25(2), 119–133. <https://research.manchester.ac.uk/en/publications/from-human-trafficking-to-modern-slavery-the-development-of-anti-/>
- 28) Lavorgna, A. (2014). Organised crime goes online. *Journal of Money Laundering Control*, 18(2), 125–138. <https://www.emerald.com/jmlc/article-abstract/18/2/153/236674/Organised-crime-goes-online-realities-and?redirectedFrom=fulltext>
- 29) Leukfeldt, R., & Yar, M. (2016). Applying routine activity theory to cyber-crime. *European Journal of Criminology*, 37(3), 263–280. https://www.researchgate.net/publication/286923434_Applying_Routine_Activity_Theory_to_Cybercrime_A_Theoretical_and_Empirical_Analysis
- 30) Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2014). Victims' voices in online grooming. *Journal of Child Sexual Abuse*, 23(5), 532–550. https://www.hrpub.org/journals/article_info.php?aid=240
- 31) Livingstone, S., & Smith, P. K. (2014). Online risks to children. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://acamh.onlinelibrary.wiley.com/doi/10.1111/jcpp.12197>



HOW CLIMATE CHANGE SHAPES MIGRATION AND HUMAN TRAFFICKING. REFLECTIONS AND OBSERVATIONS

Borislav Mavrov, Iliyana Semerdzhieva



1. Introduction

In the realities of the 21st century, characterized by deep economic interconnections and interdependencies, global connectivity through the internet and emerging technologies, as well as the growing impacts of climate change as a transboundary environmental challenge, the problems humanity faces are becoming increasingly complex. Moreover, they also increasingly intersect, often amplifying one another. Understanding these interconnections is crucial to ensuring effective policy responses.

Climate change is widely recognized as one of the most severe and long-term threats to global society. It is a multidimensional phenomenon linked to nearly every major issue. While some of these connections are well-documented and reflected in policy frameworks, others remain underexplored and insufficiently considered by decision-makers.

The relationships between climate change, migration, and human trafficking are diverse, multidirectional, and difficult to isolate from broader geopolitical, social, and ecological dynamics. Nevertheless, it is essential to disentangle this nexus, identify its most significant linkages, and assess how such analysis can inform more effective policies and practical responses to criminal networks that undermine the fundamental rights of the most vulnerable populations.

This paper offers an interpretation of the topic and represents an attempt to unpack this 3-factor nexus by incorporating the authors' perspectives. It does not claim to provide a fully comprehensive or academically novel contribution; rather, it seeks to map the interconnections among these three phenomena that have received increasing academic and political attention in recent years. The paper also attempts to examine additional linkages in order to contribute to a more nuanced understanding of this intersection, including through the application of a systems-thinking approach. Although the complexity of these phenomena and their interactions limits the scope of this overview, the paper aims to provide a foundation for further research and to support the development of more integrated and effective policy responses.



2. Historical background of the three phenomena

2.1. Migration

Migration is an inherent feature of humankind - a natural and inevitable phenomenon. As William Lacy Swing, former Director General of the United Nations' (UN) Migration Agency - the International Organization for Migration (IOM), describes it, migration is “history’s oldest and most effective anti-poverty measure, a natural human response to challenges and a facilitator of greater opportunities” (Swing, 2016).

To date, there is no legal definition of “migration” or “migrant” existing in international law. The IOM defines “migration” as “the movement of persons away from their place of usual residence, either across an international border or within a State”, and “migrant” as “a person who moves away from his or her place of usual residence, whether within a country or across an international border, temporarily or permanently, and for a variety of reasons” (IOM, 2019).

2.1.1. Environmental and climate migration

Among the various reasons that drive individuals to migrate are environmental factors and the living conditions they shape. The IOM (2019) defines “environmental migration” and “climate migration” in a similar manner, considering the latter a subcategory of the former. As is the case with “migration” as a broader term, neither concept has legal recognition, and both are used by the IOM as working definitions.

ENVIRONMENTAL MIGRATION

The movement of persons or groups of persons who, predominantly for reasons of sudden or progressive changes in the environment

CLIMATE MIGRATION

The movement of a person or groups of persons who, predominantly for reasons of sudden or progressive change in the environment



ENVIRONMENTAL MIGRATION

that adversely affect their lives or living conditions, are forced to leave their places of habitual residence, or choose to do so, either temporarily or permanently, and who move within or outside their country of origin or habitual residence.

CLIMATE MIGRATION

due to climate change, are obliged to leave their habitual place of residence, or choose to do so, either temporarily or permanently, within a State or across an international borders.

Climatic changes have always been major drivers of migration, as life on Earth has long been shaped by the climate (Tandon, 2024). Earth's unique carbon-regulated climate is the essential factor that allows water to exist in multiple states, creating the stable environment necessary for life to emerge – a balance not found on any other known planet (IPCC, 2007, p. 126). Species, including homo sapiens, evolve in response to their surrounding environments, and when conditions change, they must either adapt or relocate to areas that offer habitable conditions (Tandon, 2024). In this sense, neither environmental nor climate migration is a novel phenomenon.

2.2. Climate change

The Earth's climate has undergone numerous changes throughout its history. There have been many ice ages and warmer periods, but both have shifted and lasted for millennia (NASA, 2024). Climate change, as it is understood today within scientific, political, and public discourse, refers to anthropogenic climate change caused by excessive greenhouse gas emissions resulting from human activity in the last two centuries (Intergovernmental Panel on Climate Change [IPCC], 2007, p. 3-4). The United



Nations Framework Convention on Climate Change (UNFCCC) signed in 1992 by 198 parties was the first legal document on the international level to recognize anthropogenic climate change, defining it as “a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods”.

As reported in the Intergovernmental Panel on Climate Change (IPCC¹) report from 2007, the increase in greenhouse gas concentrations in the atmosphere over the past two centuries has occurred at both a rate and a scale that are very likely² unprecedented in at least the last 10,000 years. This has led to an increase in both frequency and intensity of sudden-onset/rapid-onset disasters (extreme weather events and extreme climate events) such as temperature extremes, heatwaves, floods, droughts, heavy precipitation, storms, and heatwaves (Seneviratne et al., 2021). At the same time, broader climate change processes are driving slow-onset environmental changes, including sea level rise, increasing temperatures, ocean acidification, glacial retreat and related impacts, salinization, land and forest degradation, loss of biodiversity and desertification (UNFCCC, 2012).

Anthropogenic greenhouse gas emissions disrupt the delicate balance of the global ecosystem, posing a risk to the living world. As climate is a fundamental condition for life on Earth, and social systems are inherently dependent on ecosystems, changes in the environment affect populations by both intensifying existing social issues and giving rise to new ones. As the impacts of climate change intensify, they are increasingly intersecting with major global challenges, including trafficking in human beings.

2.3. Trafficking in persons

Trafficking in human beings, often referred to as modern-day slavery, is one of the most severe violations of human dignity and human rights. In recent years, the number of detected victims has increased significantly at the global level. While this may partly reflect improved detection capaci-



ties of relevant institutions, it also indicates growing vulnerabilities within societies and social systems that enable this form of organized crime to persist, posing a risk to global security.

This phenomenon dates back to the earliest stages of human history, evolving from systems of forced labour in ancient societies to the large-scale Transatlantic Slave Trade (16th–19th centuries), and, following the abolition of slavery, to contemporary forms of exploitation, including human trafficking (Giovagnoni & Van Schooneveld, 2022).

“Trafficking in persons,” as defined in the Palermo Protocol³, supplementing the UN Convention against Transnational Organized Crime, refers to “the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.”

Although slavery was formally abolished worldwide by the 20th century and international efforts to combat trafficking have expanded, human trafficking persists, adapting to contemporary global dynamics and exploiting legal gaps, socio-economic vulnerabilities, and technological developments. There is growing evidence that environmental degradation and climate change intersect with and amplify existing vulnerabilities, such as poverty and climate-induced migration, thereby increasing the risk of affected populations being exploited and trafficked.



3. The nexus between climate change, migration, and human trafficking

3.1. Terms used in the context of climate mobility

Climate-induced movement of people has led to the use of the terms “climate migrant”, “climate refugee”, and “displaced person” in public discourse, academic literature, the media, and sometimes even policy (in some regions), often in an interchangeable manner. However, these terms differ significantly in both meaning and legal status.

3.1.1. Climate refugees

The term “climate refugee” is not recognized under international law. The 1951 Refugee Convention and its 1967 Protocol, which provide the internationally recognized definition of a refugee⁴ do not include environmental or climate-related factors as grounds for refugee status. Initially, the United Nations High Commissioner for Refugees (UNHCR) has criticized the term “climate refugees” as it blurs the boundaries between the definition of refugees according to the 1951 Convention and other popular notions of refugees in public discourse (Apap & Harju, 2023). Later, in 2019, the Head of the Migration, Environment and Climate Change (MECC) Division at the IOM - Dina Ionesco - argued that adding “climate refugees” to the 1951 Convention would not only weaken it, but it would also exclude from aid and support climate-displaced people who could often be unable to prove that their forced displacement is due to the changing climate and its impacts (Ionesco, 2019).

At the European level, climate change has been recognized in the context of the European Green Deal as a threat multiplier and a driver of instability, contributing to migration and population displacement (European Commission, 2019). In 2018, the European Commission proposed the establishment of an asylum, migration and integration fund aimed at addressing the root causes of irregular migration, including under-



development, demographic pressures, limited economic opportunities, climate change, and inequality. This initiative is linked to the New Pact on Migration and Asylum from 2020, which seeks to strengthen asylum systems and improve the integration of migrants. However, the Pact does not recognise climate change as a legal ground for migration or as a valid basis for asylum claims. Although a number of developing countries have called for the recognition of climate migrants as refugees, some EU Member States have not supported this approach. Instead, the EU has primarily focused on addressing the root causes of climate-induced migration, promoting global climate action - for example, through the European Green Deal, as well as through the ongoing implementation of the EU Biodiversity Strategy for 2030, which seeks to enhance resilience to the impacts of climate change (Apap & Harju, 2023).

3.1.2. Internally displaced persons

Another term used in the context of climate-induced mobility is “internally displaced person” (IDP). IDPs are “persons or groups of persons who have been forced or obliged to flee or to leave their homes or places of habitual residence, in particular as a result of or in order to avoid the effects of armed conflict, situations of generalized violence, violations of human rights or natural or human-made disasters, and who have not crossed an internationally recognized state border.”

The definition of an IDP is set out in the UN Guiding Principles on Internal Displacement. The latter constitute the main international framework for the protection of such individuals. However, they are not legally binding, although their authority has been widely recognized, particularly as they draw on international humanitarian and human rights law.

The main difference between a refugee and an IDP is that IDPs remain citizens/habitual residents of their own countries and as such, they are entitled to all the rights and guarantees. Therefore, the primary responsibility for IDP protection remains to national authorities.



3.1.3. Climate migrants

Even though climate migration is predominantly internal, some forcibly displaced people cross international borders, thereby becoming externally displaced. Despite being a recurring topic in international negotiations, the lack of an official definition and legal recognition contributes to limited protection for affected individuals, which in turn deepens their vulnerabilities (Apap & Harju, 2023).

As noted above, a climate migrant is a person who is compelled or chooses to leave their habitual place of residence, either temporarily or permanently, within a state or across international borders, primarily due to sudden or gradual environmental changes associated with climate change.

Two main forms of human mobility can be distinguished depending on the nature of environmental change. Sudden-onset events (floods, storms, and wildfires) tend to result primarily in internal displacement, placing affected populations within the category of internally displaced persons (IDPs). In contrast, slow-onset processes (rising temperatures, sea-level rise, etc.) are more often associated with migration, which represents a broader category encompassing both internal and cross-border movement. Migration may be either forced or voluntary, as individuals and households respond to both immediate shocks and gradually deteriorating living conditions (Tandon, 2024). In this sense, migration can be understood as the broader category, within which internal displacement represents a specific subset.

For the purposes of this paper, the term “climate migration” will be used to encompass both internal and cross-border displacement.

3.2. Climate change impacts on socio-ecological systems

Climate change (both in the form of gradual environmental changes and extreme weather events) has a profound impact on socio-ecological systems⁵. The International Institute for Environment and Development



(IIED), which conducted empirical research on the climate change-migration-human trafficking nexus in two districts in India, reports a range of impacts that exacerbate pre-existing vulnerabilities among affected populations, contributing to migration and, subsequently, increasing the risk of trafficking.

These impacts include:

- anomalies in rainfall patterns and increased droughts, reducing agricultural productivity; loss of forests, which can reduce groundwater levels and subsequently affect agricultural production; changing weather conditions that increase disease prevalence and insect infestations, drastically affecting yields; reduced availability of indigenous foods from forests and local water bodies; all of the aforementioned leading to food insecurity and economic hardship;
- a decline in natural resources on which communities depend for economic activities and livelihoods;
- changes in food chains - for example, wild animals feeding on resources used by communities, resulting in loss of income;
- water scarcity due to extended dry spells, which creates difficulties in meeting basic needs such as drinking, cooking, bathing, and cleaning, and also affects agriculture and other water-dependent economic activities;
- losses and damage to infrastructure, particularly during extreme weather events (Bharadwaj et al., 2022).

These examples illustrate how deeply interconnected ecological and social systems are, and how environmental disruptions translate into significant challenges for local communities. They demonstrate the strong dependence of social systems on ecosystems, implying that environmental degradation must be addressed with greater urgency. If left unaddressed, such impacts not only undermine basic human needs but also human rights, contribute to insecurity and loss of life, and create opportunities for criminal networks to exploit heightened vulnerabilities.



3.3. The impact of climate change on human mobility

Climate change is largely recognized as a factor that shapes human mobility in the present day. However, as migration is a complex phenomenon, it is often difficult to identify a single factor driving individuals or households to migrate, whether internationally or within a state. Climate change interacts with a range of other drivers – including economic, political, demographic, social, and environmental factors – making migration decisions inherently multi-causal (Ionesco, 2019). However, climate change is increasingly emerging as a significant driver of human mobility, often characterized as a threat multiplier – a factor that exacerbates existing vulnerabilities.

One clear indicator of this trend is the rising number of people internally displaced by climate-related events (Bharadwaj et al., 2022). According to the Global Report on Internal Displacement, 9.8 million people were displaced by disasters in 2024, resulting in 45.8 million internal displacements. The latter figure indicates that many individuals were displaced multiple times, often for short periods. Notably, the number of disaster-related displacements in 2024 was nearly double the annual average of the past decade (The Internal Displacement Monitoring Centre, 2025).

Although climate migration is predominantly internal, some forcibly displaced individuals cross international borders, thereby becoming externally displaced (Apap & Harju, 2023). The fact that climate change is not yet recognized under international law as a ground for seeking asylum, the lack of data on externally displaced people, combined with the tendency of climate migrants to rely on irregular migration pathways, makes it difficult to fully assess the impact of climate change on human mobility. In a worst-case scenario, up to 1.2 billion people are predicted to be displaced by 2050 due to natural disasters and other ecological threats (Institute for Economics and Peace, 2020).



Climate-driven migration is associated with severe forms of exploitation in at least three ways: (i) slow-onset disasters, including gradual environmental changes such as droughts and crop failures; (ii) rapid-onset disasters, such as floods and cyclones; and (iii) the combined effects of conflict and climate-related events (Bharadwaj et al., 2022).

3.3.1. Sudden-onset disasters

Sudden-onset disasters are triggered by hazardous events that emerge quickly or unexpectedly. Climate-related sudden-onset disasters are, for example, floods, cyclones, tornadoes, landslides, wild fires, etc. Depending on their severity and the affected populations' vulnerabilities and adaptive capacity, they could result in temporary or protracted displacement (United Nations High Commissioner for Refugees [UNHCR], n.d.). This is because sudden-onset events can cause extensive loss and damage to crops, livestock, land, property, equipment, and even homes. In these circumstances, communities often have limited or no options for in-situ adaptation, making migration the only viable means of survival, especially for people without safety nets who are instantly plunged into poverty (Bharadwaj et al., 2022).

3.3.2. Slow-onset disasters

Slow-onset events evolve gradually, either from incremental changes occurring over many years or from an increased frequency or intensity of recurring events (UNHCR, n.d.). Examples include recurrent droughts, coastal erosion, sea-level rise, desertification, and glacial retreat, all of which threaten natural resource-based livelihoods such as agriculture, livestock, and fisheries (Bharadwaj et al., 2022). Gradual environmental changes, particularly when irreversible, undermine ecosystems and resource availability, thereby contributing to food insecurity and long-term economic instability (Brouwer, 2025). They undermine people's ability to sustain their livelihoods, often leading to increased debt and poverty. As a result, households may be motivated or forced to consider migration in



search of better economic opportunities. Migration can thus serve as a coping strategy that enables the diversification of livelihoods (Bharadwaj et al., 2022). This is enhanced by the fact that usually disaster risk reduction responses and social protection programmes are focused primarily on sudden onset-events, because of their higher visibility and perceived urgency (Brouwer, 2025).

3.3.3. The intersection of climate change and conflict

Climate change has been widely recognized as a threat multiplier by scientists, civil society, and policymakers, including in relation to peace and security. The IOM also states that climate change can cause or least contribute to situations of conflict and instability, which then trigger migration flows (IOM, 2016). However, the extent of its impact and the nature of the risks it poses remain subjects of ongoing debate. The fact that the United Nations Security Council convened a meeting just two months after 197 parties to the UN Climate Change Convention agreed on a concrete pathway for implementing the 2015 Paris Agreement (United Nations, n.d.) underscores the growing international concern over the security implications of climate change and highlights its increasing prominence on the global political agenda.

The following example illustrates how complex, intersecting factors can make it difficult to attribute outcomes to a single driver. In the case of the Syrian Civil War that caused one of the worst refugee crises, the conflict has been framed as a “climate conflict” due to a severe drought between 2007 and 2009. However, a report by the United Nations University Institute for Water, Environment and Health challenges this widely circulated narrative, arguing that the crisis was driven primarily by long-term governance failures and maladaptive agricultural and economic policies rather than climate change alone.

Drawing on satellite data and field research, the study shows that rural collapse and farmland abandonment began well before the drought, largely



as a result of subsidy cuts, structural inequalities, and unsustainable farming practices. Although the drought was severe, Syria's agricultural sector demonstrated resilience and even recovered shortly before the outbreak of war. Migration prior to 2011 was largely a common coping strategy, but it became forced and permanent only after the onset of violent conflict.

The report concludes that labeling the Syrian war as a “climate conflict” oversimplifies a complex reality and diverts attention from deeper political and economic drivers, particularly poor governance (Von der Kammer et al., 2025).

While the conflict cannot be directly attributed to climate change, these governance failures were closely tied to the mismanagement of natural resources and a disregard for socio-ecological systems, highlighting how the neglect of human-environment interdependencies can deepen vulnerability.

3.4. The relation between climate change and trafficking in persons

Climate change increases the risk of human trafficking both in origin areas affected by environmental stress and during migration. Despite the fact that, the effect of sudden-onset disasters on trafficking is often more clearly evident in comparison to the impact of slow-onset disasters (IOM, 2017), this activity has been shown to increase in areas affected by gradual processes as well as in those impacted by rapid-onset events (Bharadwaj et al., 2022).

Depending on the context, sometimes slow-onset events could even lead to higher rates of human trafficking. For example, research by the International Institute for Environment and Development (IIED) indicates that trafficking rates were significantly higher in a district in an Indian state affected by slow-onset climate events compared to one impacted by rapid-onset disasters. This disparity can be attributed to the fact that slow-onset disasters typically receive less attention than sudden events. In



such cases, moderate droughts must be addressed by state governments using their own resources, which can delay official recognition. Consequently, some states neglect declaring drought conditions until they become severe enough to qualify for federal assistance. As a result, many droughts go unreported or are declared too late, pushing communities into distress migration as they struggle to sustain their livelihoods and access basic necessities (Bharadwaj et al., 2022).

3.4.1. Recruitment at affected (source) areas

Criminal networks conducting trafficking in persons target affected regions and take advantage of vulnerable individuals who are in search of opportunities to restore their lives after disasters, being aware that such people are likely to be more prone to resort to high-risk behaviours and potentially dangerous coping strategies. For example, after Cyclone Sidr in 2007 in Bangladesh, research showed that criminal networks began to operate in the affected region (Munns & Katz, 2023).

Affected populations out of desperation could also see as an option colluding with criminal actors. For example, there have been cases of men selling their wives/other female relatives or parents selling their children (also a form of trafficking in persons) – seen as coping strategies in the context of severe impacts of a changing climate (Bharadwaj et al., 2022).

Even though trafficking is associated mostly with mobility, there are disaster-affected people are unwilling or unable to move. This involuntary immobility can leave populations highly vulnerable, as the ability to move is often a crucial coping strategy in response to livelihood loss (Brower, 2025).

3.4.2. Recruitment during migration

Apart from targeting the source areas of forcibly displaced populations, individual recruiters and criminal networks target migrant destinations as well – e.g., in the urban slums displaced people are relocated to or in refugee camps established to shelter internally displaced people. Usually



these camp-like settings are overcrowded, lack social cohesion, security, as well as access to social services, offer few employment opportunities, and are characterized by competition for resources like food or water. Recruiters/traffickers integrate into the camp environment, earn trust among inhabitants, which helps them identify potential victims. Especially when displaced people are forced to spend longer periods of time in these settings, they become increasingly desperate, and fall victims of forced labour, debt bondage, sexual exploitation, or are forcibly married (Munns & Katz, 2023).

3.5. Vulnerability of climate-induced migrants to human trafficking

In a publication dedicated to the nexus between climate change and human trafficking, the International Organization for Migration (2017) states that “migrants who report war, conflict, or natural disasters as the main reason for leaving their places of origin are more likely to be vulnerable to exploitation and human trafficking during their journey than those who migrate for other reasons.”

There are multiple factors underlying the vulnerability of climate migrants to human trafficking, both during transit and at their destination. Some of the most significant among them are as follows:

Firstly, the nexus between climate change, migration, and trafficking in persons is most evident among populations living in precarious or uncertain economic conditions (e.g. poverty, unemployment, high indebtedness, lack of education, etc.). It is not necessarily the areas most exposed to environmental and climate hazards that experience the most severe impacts leading to migration and trafficking, but rather those where communities lack the capacity to cope with these impacts and where populations already face economic hardship and limited resources to respond to extreme weather events (Munns & Katz, 2023). Consequently, climate change amplifies existing economic vulnerabilities, increasing suscepti-



bility to exploitation and making affected populations more likely to resort to high-risk coping strategies as irregular migration that may expose them to human trafficking.

However, it is not only economic hardship and loss of shelter that drive people to adopt such coping strategies. Factors such as loss of access to essential infrastructure, including healthcare, education, and social services, as well as the erosion of social networks, cultural heritage, and community support, can also play a significant role (Brower, 2025).

An important factor is the nature of climate change impacts, particularly extreme weather events. Climate-induced migration is often categorized as a form of distress migration, placing affected individuals in situations characterized by a lack of alternative options (Avis, 2017). Additionally, the significant strain on livelihoods accelerates migration decision-making among affected populations. This often results in unplanned/poorly planned migration as a risky coping strategy, thereby increasing vulnerability to exploitation and the risk of human trafficking (Brennan & Yea, 2025). Apart from the urgency of displacement, disaster-affected populations often face economic constraints, which contribute to their reliance on irregular and unsafe migration pathways that are perceived cheaper than regular migration channels (IOM, 2017).

Therefore, climate-induced migration is largely unregulated – individuals are not formally registered, which makes the tracking of their movement difficult (Bharadwaj, 2022). By crossing international borders irregularly (being undocumented), individuals have limited access to government support, legal and labour protection in transit and destination countries (Munns & Katz, 2023). Together these factors increase vulnerability to exploitation, and consequently, undocumented migrants constitute a significant share of victims of human trafficking (World Bank, 2023).

As a coping mechanism, individuals affected by climate-related disasters, could seek assistance from migrant smugglers. However, this activity increases the chances of smuggled people to become victims of trafficking (IOM, 2017).



3.5.1. Other contributing factors

The role of unscrupulous recruitment agents in facilitating labour migration represents an additional contributing factor. These intermediaries often enable movement from rural communities to areas with a high demand for low-cost labour. Migrants frequently lack formal employment contracts or written agreements with employers or intermediaries, which limits their access to legal protection (Bharadwaj, 2022). At the same time, some recruitment practices have been linked to exploitative outcomes, including forced labour.

For example, in the Sundarbans, after climate change-related disasters, it was reported that labour recruiters and contractors have exploited the unstable conditions of affected communities by recruiting individuals - particularly women and children - through deceptive promises of employment or marriage. Reflecting existing gendered divisions of labour, many women and girls were subsequently trafficked into sectors with high demand, such as domestic work, the sex industry, and forced marriage, while boys were trafficked for forced labour across various sectors (Molinari, 2017).

Another factor that plays an important role is the already existing human trafficking activity in the affected regions. Most of them are low-income populations who are already vulnerable to and become victims of trafficking. The law enforcement systems of the respective governments already struggle to deal with trafficking and other types of modern slavery in “normal” times, and in times during and after a disaster, it becomes even more difficult and many of these populations are left unprotected.

3.5.2. Socio-political factors on the national level

It is important not to overlook socio-political factors when addressing climate change and its related impacts. Lack of or inadequate support systems (disaster management strategies and social protection programmes) also lead to deepening of vulnerabilities, which decreases resilience and



adaptive capacity of societies. The vast majority in low- and middle-income countries usually have insufficient resources and infrastructure to provide the humanitarian, economic and social protection for forcibly displaced persons (Munns & Katz, 2023). At the same time, absence of or inadequate early warning systems for climate-related hazards play a crucial role in failure of socio-political systems to safeguard livelihoods, lives, and assets. (Bharadwaj, 2022). Therefore, malfunctioning of the rule of law and poor governance structures also play a role in both prevention and post-disaster management (Munns & Katz, 2023).

For example, evidence from the two studied districts in India, which exemplify the nexus between climate change, migration, and human trafficking, shows that affected populations often lack adequate strategies and resources to manage climate-related risks. This includes insufficient infrastructure to cope with floods and cyclones, limited access to facilities such as flood shelters, irrigation systems, community centres, and reliable drinking water sources, as well as inadequate provision of relief materials following disasters. In such contexts, some of the most vulnerable individuals have been found to resort to high-risk coping strategies – irregular migration that resulted in trafficking (Bharadwaj, 2022).

3.5.3. Gender-specific dimensions

According to UNICEF, climate change heightens the likelihood that girls could be forced into unsafe migration or displacement pathways, increasing their exposure to risks of modern slavery. Girls are particularly vulnerable to trafficking, especially during and after extreme weather events. These risks are further intensified when they are responsible for collecting essential resources such as food, water, and firewood, or when they reside in temporary shelters or refugee camps (Pegram & Colon, 2020).

At the same time, research from the Sundarbans and other regions in India indicates that, in post-disaster contexts, higher rates of gender-based violence, exploitation, and human trafficking - particularly affecting women and girls - have been reported. These outcomes are linked to



factors such as family fragmentation and stress, loss of livelihoods and support networks, disruption of social norms and protective structures, displacement into insecure disaster relief camps, and heightened physical and socio-economic vulnerability (Molinari, 2017).

The IOM (2017) also suggests, based on existing evidence, that women and female-headed households are particularly vulnerable to trafficking, as well as children who are displaced or orphaned during climate-related disasters. However, the organization also highlights the need for further research to better understand differences in vulnerability to human trafficking among men, women, boys, and girls in the context of a changing climate.

3.6. Examples of the nexus and existing evidence

There has been growing empirical evidence about the links between climate change, migration and human trafficking. Climate change induces high-risk migratory patterns to both rapid and slow-onset disasters, which exacerbates affected populations' vulnerability to trafficking and slavery-like practices (Munns & Katz, 2023).

3.6.1. The Asia-Pacific region

In a dedicated publication, the IOM (2017) outlines examples from the Asia-Pacific region that illustrate the nexus between climate change, human mobility and trafficking in persons. The region is the world's most populous region, with more than 4.2 billion people. It is also characterized by high levels of human mobility, including both internal and international migration, as well as regular and irregular migration flows, including human trafficking. Migration within the region is predominantly internal, often taking the form of rural-to-urban movement. Human trafficking frequently occurs along these same routes and is carried out by organized criminal networks, with major destination countries including India, Malaysia, and Thailand. Irregular labour migration is often associated with forms of exploitation commonly linked to human trafficking.



At the same time, the region is among the most vulnerable to the impacts of climate change, being exposed to a wide range of natural hazards. These include both sudden-onset events, such as cyclones and floods, and slow-onset processes, such as droughts and sea-level rise. These climate-related events significantly influence human mobility, with millions of people displaced across the region each year. A notable trend is the increasing number of people displaced for prolonged periods, often forced to live in camps or camp-like settings. Environmental and climatic changes can therefore trigger high-risk forms of migration, driven by both sudden and slow-onset events.

There is also documented evidence of increased risks of human trafficking during and after natural disasters, including the Indian Ocean tsunami (2004), Cyclone Sidr in Bangladesh (2007), and Typhoon Haiyan in the Philippines (2013). In such contexts, criminal networks have been found to target affected populations, particularly vulnerable groups such as children, widows, and individuals seeking to migrate for employment. In some cases, even entire families have been targeted, and especially female-headed households have been exposed to heightened risks of exploitation.

3.6.2. Geographical scope of existing evidence and EU Implications

Certain regions of the world have proven to be particularly vulnerable to the increasing frequency and intensity of climate-related disasters, as well as to human trafficking. These include lower- and middle-income countries in South Asia, East Asia and the Pacific, Sub-Saharan Africa, and the Middle East. These regions are characterized by high exposure to natural hazards, limited capacity for adaptation, and large populations dependent on natural resources (Brouwer, 2025). As most existing empirical evidence on the climate change-migration-human trafficking nexus is based on research conducted in these regions, findings may vary in other geographical contexts.



While certain regions are disproportionately affected, no country or region is immune to either climate change or trafficking in persons, as both are global phenomena. Evidence suggests that climate change can exacerbate vulnerabilities across diverse socio-economic contexts, although its impacts are often most visible in regions already facing structural challenges.

The afore-mentioned research by the IIED demonstrates that this dynamic is not limited to traditionally vulnerable regions. A comparative study of two districts in India (Palamu and Kendrapara) shows that even relatively prosperous and stable regions can become highly vulnerable under increasing climate stress. Kendrapara, once among the most fertile and economically stable districts in Odisha, historically attracted migrants due to its productive land and favourable conditions. In contrast, migration in the region has emerged as a relatively recent phenomenon, driven by the growing impacts of climate change, including more frequent cyclones, flooding, sea-level rise, and land degradation. These changes have undermined livelihoods, leading to declining incomes, unemployment, and rising indebtedness (Bharadwaj, 2022).

Despite higher levels of literacy, better infrastructure, and stronger economic conditions compared to Palamu, populations in Kendrapara have also become increasingly vulnerable. In both districts, it is the most vulnerable groups who are disproportionately affected and are more likely to fall victims to trafficking. This highlights that while pre-existing socio-economic conditions shape vulnerability, climate change can act as a powerful stress multiplier, extending risks even to populations that were previously relatively secure.

In this context, although there is currently no empirical evidence directly linking climate change, migration, and human trafficking within the EU, a briefing from the European Parliamentary Research Service suggests that the EU may need to reconsider its perspective on climate-related mobility - not only as a destination for displaced populations from abroad, but also as a region experiencing internal climate displacement.



While current policy frameworks, such as the European Green Deal, primarily focus on addressing the root causes of climate change, insufficient progress in emissions reduction may necessitate greater attention to the impacts of climate change, including climate-related migration (Apap & Harju, 2023). Migration, on its end, could possibly heighten vulnerabilities among affected regions and populations, thereby creating conditions that could be exploited by criminal networks, including those involved in human trafficking.



4. Additional dimensions of the climate change - human trafficking relationship

Migration does not inherently lead to trafficking; however, without proper regulation, it can increase vulnerability to exploitation. At the same time, migration can have several positive effects on households. It can improve health and nutrition, increase purchasing power, and diversify income. Migration may also enhance economic security, expand access to education and employment opportunities, and help households cope with climate-related stress, enabling them to move out of cycles of debt and poverty while strengthening their capacity to save and invest (Bharadwaj et al., 2022).

These findings suggest that migration is not inherently negative; rather, it needs to be safe, voluntary, and well-regulated to ensure that individuals are protected and able to make informed choices.

4.1. Climate Change and labour exploitation

Climate change not only contributes to increased vulnerability to trafficking, but also exacerbates exploitative labour conditions. As highlighted by Brennan and Yea (2025), already precarious forms of work can more easily shift into situations of extreme exploitation or trafficking in the context of the climate crisis. In many regions, working conditions are deteriorating due to rising temperatures, environmental degradation, and the increasing frequency of extreme weather events, in some cases becoming even life-threatening.

At the same time, climate change further worsens the conditions experienced by individuals already subjected to exploitation or trafficking. Victims of trafficking, who often work in informal or unregulated sectors such as agriculture, construction, or fisheries, are particularly exposed to environmental hazards. As climate impacts intensify, these workers may face longer hours under extreme weather conditions, reduced protections, and increased physical risk, deepening their vulnerability (Brennan & Yea, 2025).



4.2. A systems perspective: feedback loop dynamics between climate change and trafficking in persons

Human trafficking and climate change are also linked through non-linear relationships that can form reinforcing (positive) or balancing (negative) feedback loops.

As discussed in this paper, climate impacts increase vulnerability to trafficking. At the same time, many sectors associated with forced labour and exploitation - such as intensive agriculture, cattle ranching, fisheries, forestry, mining, and construction - are significant contributors to environ-

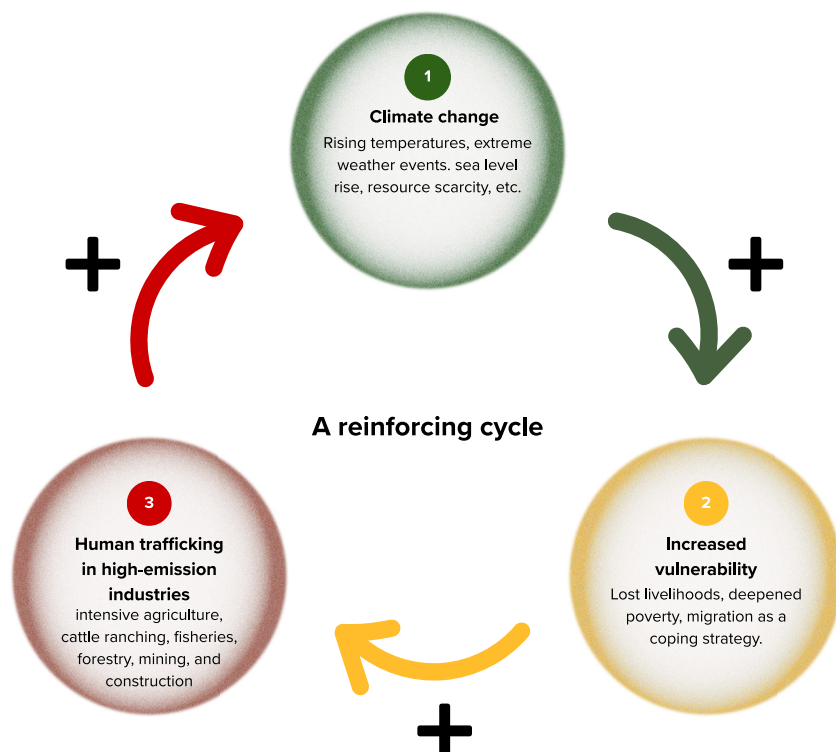


Figure 1 – Example of a positive feedback loop (high-emission industries)



mental degradation and climate change. In this way, exploitative practices not only arise from climate-induced vulnerability but also contribute to further environmental damage, which in turn exacerbates climate change impacts. This creates a reinforcing cycle in which climate change drives vulnerability and exploitation, while exploitation further intensifies environmental degradation. Human mobility in the absence of safe and regular pathways represents a key element of this nexus, acting as a major risk factor for trafficking in persons that is increasingly influenced by climate change (Brouwer, 2025).

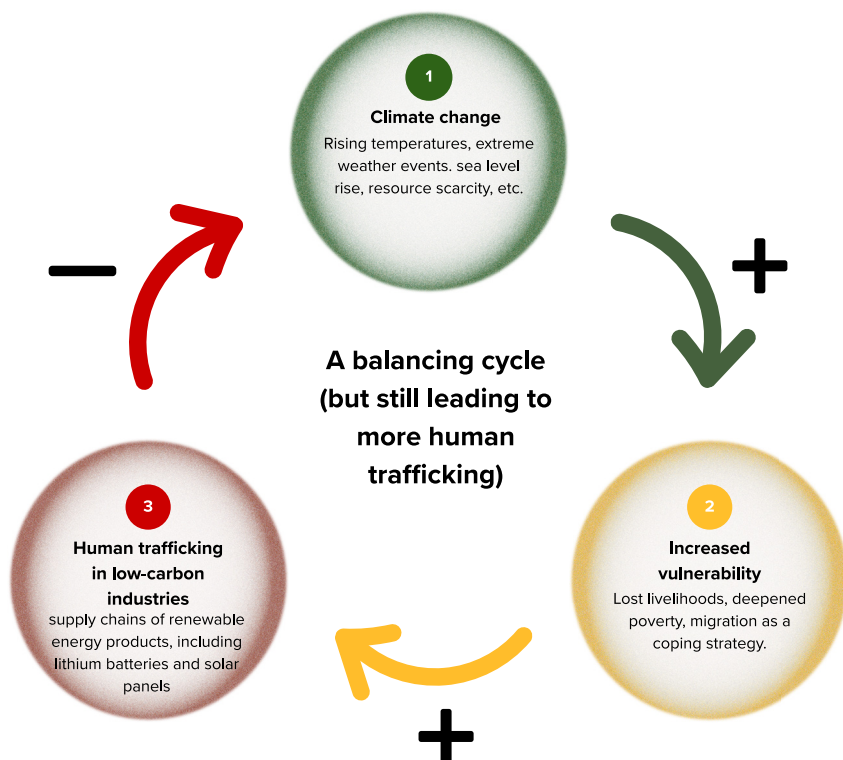


Figure 2 – Example of a negative feedback loop (low-carbon industries)



However, forced and child labour have also been identified in the supply chains of renewable energy products, including lithium batteries and solar panels, which are central to the green transition. This highlights a more complex dynamic: while these industries aim to mitigate climate change, they may still rely on exploitative labour practices (Brouwer, 2025).

In this sense, efforts to address environmental challenges do not automatically translate into positive social outcomes. Despite the balancing feedback loop being formed, rather than representing a purely beneficial or “balancing” dynamic, this reflects a broader systemic issue in which exploitation persists across both high-emission and low-carbon sectors. Regardless of whether industries contribute to climate change or aim to mitigate it, the continued presence of human trafficking and forced labour across diverse sectors underscores the global, multi-faceted nature of the problem and its deeply embeddedness within contemporary economic systems.



5. Conclusion

The nexus between climate change, migration, and trafficking in persons is becoming increasingly evident, reflecting its complexity and deep interconnections with broader social, economic, and environmental challenges. A growing body of research highlights how climate change acts as a threat multiplier, exacerbating existing vulnerabilities and creating conditions in which exploitation and human trafficking can flourish. At the same time, leading institutions, including the International Organization for Migration, emphasize that this nexus remains underexplored and insufficiently reflected in policy frameworks at both national and international levels. This highlights the urgent need for more systematic integration of these interconnections into policymaking processes.

Despite growing attention, significant research gaps remain as well. Current evidence is largely based on case studies and is geographically concentrated in regions such as South and Southeast Asia. There is a need for more large-scale, quantitative research to better understand the causal pathways linking climate change and trafficking, including the role of slow-onset environmental changes. Further research is also needed to identify which population groups are most vulnerable and under what conditions. Expanding the geographical scope of research and deepening the evidence base are essential for informing effective and targeted policy responses.

A key implication is the lack of clear definitions and legal recognition of climate-related mobility. The absence of internationally agreed terminology and protection frameworks for climate migrants contributes to gaps in protection and may push affected populations toward irregular migration pathways, thereby increasing their vulnerability to exploitation and trafficking. Addressing this gap is essential to ensure that those most affected by climate change are adequately protected. In this context, improving migration governance is crucial - not only to reduce risks but also to recognize that, when properly managed, migration can serve as a positive adaptation strategy that enhances resilience to environmental change.



At the same time, policy responses must move beyond reactive approaches and place greater emphasis on prevention by addressing the root causes of vulnerability. Since climate change amplifies pre-existing inequalities - such as poverty, gender inequality, weak governance, and environmental degradation - effective responses must focus on strengthening socio-economic resilience. This includes investing in climate-resilient infrastructure, disaster preparedness and early warning systems, social protection mechanisms, and sustainable livelihood opportunities. By reducing structural vulnerabilities, such measures can limit the conditions that traffickers exploit and reduce the likelihood that affected populations resort to high-risk coping strategies.

Closely linked to this is the need for more integrated and systemic approaches to policymaking. The complexity of the climate-migration-trafficking nexus demonstrates that these issues cannot be addressed in isolation. A systems thinking approach allows policymakers to better understand interconnections, identify reinforcing feedback loops, and anticipate unintended consequences. Such an approach also supports the development of integrated strategies that simultaneously address climate adaptation, environmental protection, migration governance, and anti-trafficking efforts.

Importantly, these findings also highlight the need to avoid oversimplification. While climate change is an important driver of vulnerability, it should not be viewed in isolation or as the sole cause of migration and trafficking. Environmental change has always been a feature of human history, and vulnerability is shaped by a broader set of socio-political and economic factors, including governance deficits, and limited institutional capacity. At the same time, it is essential to recognize that contemporary climate change is anthropogenic, and therefore closely linked to governance systems, policy choices, and patterns of economic development. Framing climate change as an abstract or independent driver risks obscuring the underlying human and institutional decisions that contribute to both environmental degradation and social vulnerability. Effective re-



sponses must therefore place greater emphasis on governance structures and accountability, ensuring that policy decisions consider their long-term impacts on both human societies and natural systems.

In an increasingly interconnected and globalized world, challenges such as climate change, migration, and human trafficking are becoming more complex and interdependent. Addressing them requires not only deeper academic understanding, but also more coordinated, forward-looking, and integrated policy action. Recognizing and responding to these interlinkages is essential to ensuring both human security and sustainable development in the face of accelerating global change.

1 The Intergovernmental Panel on Climate Change (IPCC) is widely regarded as the premier global authority on climate science.

2 In the IPCC calibrated language system, the term „very likely“ denotes a probability of occurrence greater than 90%.

3 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children

4 According to the Convention, a refugee is defined as a person who, “owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of [their] nationality and is unable or, owing to such fear, unwilling to avail [themselves] of the protection of that country; or who, not having a nationality and being outside the country of [their] former habitual residence, is unable or, owing to such fear, unwilling to return to it.”

5 The term “socio-ecological systems” refers to complex, integrated systems of people and nature, emphasizing that humans are not separate from the natural world but an inherent part of it (Berkes and Folke, 2000).



6. Resources:

1. Swing, W. L. (2016, September 19). MIGRATION IS OUR HISTORY, REALITY AND FUTURE. IOM Blog. <https://weblog.iom.int/migration-our-history-reality-and-future>
2. International organization for Migration. (n.d.). ENVIRONMENTAL MIGRATION. iom.int. Retrieved February 2, 2026, from <https://environmentalmigration.iom.int/environmental-migration>
3. International Organization for Migration. (2019). Glossary on migration (International Migration Law No. 34). https://publications.iom.int/system/files/pdf/iml_34_glossary.pdf
4. Ayesha Tandon. (2024, April 11). How does climate change drive human migration? Carbon Brief. <https://interactive.carbonbrief.org/climate-migration/index.html>
5. Intergovernmental Panel on Climate Change. (2007). Climate change 2007: The physical science basis. Contribution of Working Group I to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change (S. Solomon, D. Qin, M. Manning, Z. Chen, M. Marquis, K. B. Averyt, M. Tignor, & H. L. Miller, Eds.). Cambridge University Press.
6. UNFCCC. (2012). Slow onset events: Technical paper (FCCC/TP/2012/7). Secretariat of the United Nations Framework Convention on Climate Change. <https://unfccc.int/documents/7429>
7. Seneviratne, S. I., X. Zhang, M. Adnan, W. Badi, D. Dereczynski, A. Di Luca, S. Ghosh, I. Iskandar, J. Kossin, S. Lewis, F. Pinto, I. F. T. Pires, K. Raghavan, C. Singh, & C. U. A. (2021). Weather and climate extreme events in a changing climate. In Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [Masson-Delmotte, V., P. Zhai, A. Pirani, S. L. Connors, C. Péan, S. Berger, N. Caud, Y. Chen, L. Goldfarb, M. I. Gomis, M. Huang, K. Leitzell, E. Lonnoy, J. B. R. Matthews, T. K. Maycock, T. Waterfield, O. Yelekçi, R. Yu, & B. Zhou (eds.)]. Cambridge University Press. <https://doi.org/10.1017/9781009157896.013>



8. NASA. (2024, October 23). Evidence - NASA Science. NASA Science. <https://science.nasa.gov/climate-change/evidence/>
9. Ionesco, D. (2019, June 6). Let's talk about climate migrants, not climate refugees. United Nations Sustainable Development. <https://www.un.org/sustainabledevelopment/blog/2019/06/lets-talk-about-climate-migrants-not-climate-refugees/>
10. Apap, J., & Harju, S. (2023). The concept of "climate refugee." In <https://www.europarl.europa.eu/>. European Parliamentary Research Service. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)698753](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698753)
11. International Labour Organization, Walk Free, & International Organization for Migration. (2022). Global estimates of modern slavery: Forced labour and forced marriage. International Labour Organization. <https://www.ilo.org/publications/global-estimates-modern-slavery-forced-labour-and-forced-marriage-1>
12. Anti-Slavery International. (2025, December 9). Migration and trafficking. [antislavery.org. https://www.antislavery.org/what-we-do/migration-and-trafficking/](https://www.antislavery.org/what-we-do/migration-and-trafficking/)
13. European Commission. (2019). The European Green Deal (COM/2019/640 final). <https://eur-lex.europa.eu/legal-content/EN/TX-T/?uri=celex:52019DC0640>
14. Bharadwaj, R., Chakravarti, D., Karthikeyan, N., Hazra, S., Daniel, U., Topno, J., & Abhilashi, R. (2022). Climate change, migration and vulnerability to trafficking. International Institute for Environment and Development. <https://www.iied.org/20936iied>
15. Pegram, J., & Colon, C. (2020). Are climate change policies child-sensitive? United Nations Children's Fund (UNICEF). https://www.unicef.org/media/72561/file/Are-climate-change-policies-child-sensitive-2020_0.pdf
16. International Organization for Migration. (2017). THE CLIMATE CHANGE–HUMAN TRAFFICKING NEXUS. <https://publications.iom.int/books/climate-change-human-trafficking-nexus>



17. Brouwer, J. (2025). Human Mobility and Vulnerability to Trafficking in Persons in the Context of Climate Change, Environmental Degradation, and Disasters. Assessment of the Available Evidence. International Organization for Migration. <https://migrantprotection.iom.int/en/resources/report/human-mobility-and-vulnerability-trafficking-persons-context-climate-change>
18. Munns, N., & Katz, G. (2023). Climate- and conflict-induced migration and modern slavery: challenges and opportunities for action. Justice and Care. https://justiceandcare.org/app/uploads/2023/03/Justice-and-Care-Issue-Brief_Migration_Climate-and-Conflict_Mar23.pdf
19. The Internal Displacement Monitoring Centre. (2025). Global Report on Internal Displacement. In <https://api.internal-displacement.org>. https://api.internal-displacement.org/sites/default/files/publications/documents/idmc-grid-2025-global-report-on-internal-displacement.pdf?_gl=1*hzls2q*_ga*NzYyMTU4Njc1LjE3NzU2NzU0MzE.*_ga_PKVS5L6N8V*czE3NzU2NzU0MzEkzbEkZzAkdDE3NzU2NzU0MzEkajYwJGwwJGgw
20. Molinari, N. (2017). Intensifying Insecurities: The impact of climate change on vulnerability to human trafficking in the Indian Sundarbans. *Anti-Trafficking Review*, 8. <https://doi.org/10.14197/atr.20121784>
21. World Bank. (2023). WORLD DEVELOPMENT REPORT 2023. <https://openknowledge.worldbank.org/server/api/core/bitstreams/c1522c0b-6d35-491d-a008-e76535b53291/content>
22. Avis, W. (2017). Scoping study on defining and measuring distress migration. Governance and Social Development Resource Centre. <https://www.gsdr.org/wp-content/uploads/2017/04/HDR1406.pdf>
23. Institute for Economics and Peace. (2020). Over one billion people at threat of being displaced by 2050 due to environmental change, conflict and civil unrest [Press release]. <https://www.economicsandpeace.org/wp-content/uploads/2020/09/Ecological-Threat-Register-Press-Release-27.08-FINAL.pdf>
24. United Nations. (n.d.). Climate change recognized as ‘threat mul-



tiplier', UN Security Council debates its impact on peace | COMMISSION DE CONSOLIDATION DE LA PAIX. <https://www.un.org/peacebuilding/news/climate-change-recognized-%E2%80%9998threat-multiplier%E2%80%99-un-security-council-debates-its-impact-peace>

25. Berkes, F., & Forke, C. (2000). Linking social and ecological systems for resilience and sustainability. Cambridge University Press. https://assets.cambridge.org/97805217/85624/excerpt/9780521785624_excerpt.pdf

26. Internal Displacement Monitoring Centre. (n.d.). Disasters and climate change. www.internal-displacement.org. <https://www.internal-displacement.org/disasters-and-climate-change/>

27. United Nations High Commissioner for Refugees. (n.d.). Master glossary of terms. www.unhcr.org. <https://www.unhcr.org/glossary>

28. Von der Kammer, R., Dinc, P., & Eklund, L. (2025, December 18). THE DROUGHT-MIGRATIONCONFLICT NEXUS. [unu.edu](https://collections.unu.edu/eserv/UNU:10394/INWEH_Report_Drought_Migration_Conflict_2025.pdf). https://collections.unu.edu/eserv/UNU:10394/INWEH_Report_Drought_Migration_Conflict_2025.pdf

29. Giovagnoni, B., & Van Schooneveld, A. (2022, January 25). The History of Human Trafficking. The Exodus Road. <https://theexodusroad.com/history-of-human-trafficking>

This analytical article has been developed as part of the project “Capacity building through exchange of good practices and research in the security domain” No. BG65ISPR001-3.004-0002, Contract No. 812108-68-02.10.2024, funded by the Program of the Republic of Bulgaria under the Internal Security Fund 2021-2027.

The content of this material does not reflect the official opinion of the European Union and the Responsible Managing Authority. Responsibility for the information and views expressed in the document lies with its author and the European Institute Foundation.



**Co-funded by
the European Union**



Address:	101 "G. S. Rakovski" St, 1000 Sofia
Telephone:	+359 2 988 64 10
Email:	office@europe.bg
Web:	https://www.europeaninstitute.bg/en
Facebook:	Европейски институт, European Institute