PRE-RIGHTS

PRE-RIGHTS PROJECT:
Assessing impact and performance
of preventive measures
on EU Directives and Framework Decisions.

D.3.2 Hybrid Investigations and Intelligence Data Gathering

PARTNERS

CEI
CENTRAL EUROPEAN INITIATIVE

CSD
CENTER FOR THE STUDY OF DEMOCRACY

AGENFOR
INTERNATIONAL

L-Università ta' Malta

IPS
INNOVATIVE PRISON SYSTEMS

Die Senatorin für Justiz und Verfassung
Freie Hansestadt Bremen

KEMEA

ROMANIAN-AMERICAN UNIVERSITY

GRAPHIC DESIGN
Studio Mark, Trieste

2022

Project

ACRONYM	PRE-RIGHTS
TITLE	Hybrid Investigations and Intelligence Data Gathering
COORDINATOR	InCE Iniziativa Centro Europea – Segretariato Esecutivo
REFERENCE	831616
CALL	JUST-JCOO-AG-2018
TYPE OF ACTION	JUST-AG
CONSORTIUM	1. InCE Iniziativa Centro Europea – Segretariato Esecutivo (InCE-SE), Italy 2. Center for the Study of Democracy (CSD), Bulgaria 3. Agenfor International Foundation (AGENFOR), Italy 4. Universita TA Malta (UOM), Malta 5. Qualify Just - IT Solutions and Consulting LDA (IPS), Portugal 6. Bremen Senate of Justice and Constitution (Bremen MoJ), Germany 7. Kentro Meleton Asfaleias (KEMEA), Greece 8. Universitatea Romano Americana Asociatie (RAU), Romania

Deliverable

NUMBER	Deliverable 3.2
TITLE	Hybrid Investigations and Intelligence Data gathering
LEAD BENEFICIARY	Center for the Study of Democracy (CSD)
WORK PACKAGE	3
DISSEMINATION LEVEL	PU
DUE DATE	31 May 2022
AUTHORS	Tatyana Novossiolova

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

TABLE OF CONTENTS

Introduction 9

Mapping the Phenomenon of Terrorism 11

Psychology of Terrorism and the Process of Violent Radicalisation 11

Figure 1: Four-stage process of ideological development 14

Box 1: Defining radicalisation and extremism 17

Terrorist Offences and Offences Related to Terrorist Activities 20

Data Collection in Counter-Terrorism 23

Preventing Terrorist Offences: The Role of Policing 23

Box 2: Trends in Crime Prevention 25

Countering radicalisation in cyberspace 28

Box 3: Behavioural indicators for terrorist activity online 32

Tackling terrorism financing 33

Box 4: Applying new technologies for AML/CTF 39

Intercepting terrorist perpetrators and suspects 40

Box 5: PNR Directive and data collection 41

Figure 2: Trends in biometric data collection for counter-terrorism 43

Box 6: Facial recognition technology in law enforcement: a fundamental rights perspective 46

Box 7: International Principles on the Application of Human Rights to Communications Surveillance 48

Box 8: AI prediction in counterterrorism: cost-benefit considerations 51

Community-based Approaches for Preventing Violent Radicalisation 52

Box 9: Tackling terrorism – the role and responsibilities of local authorities 53

Conclusion 57

Introduction

This report examines the issue of hybrid investigations and intelligence data gathering for the purpose of terrorism prevention. Terrorism here is understood within the scope of EU Directive 2017/541. Terrorist plots are difficult to uncover and pre-empt due to at least four reasons. First, acts of terrorism can be motivated by different political or religious ideologies. For example, Europol has developed an indicative typology of terrorism that covers five broad categories: jihadist terrorism; ethno-nationalist and separatist terrorism; left-wing and anarchist terrorism; right-wing terrorism; and single-issue terrorism (e.g. violent activism regarding animal rights).[1] Second, terrorism is characterised by the use of indiscriminate violence or threat thereof which includes targeting civilians. Third, terrorist groups and networks operate in a clandestine manner and deploy different tactics for attracting supporters and recruiting operatives. And fourth, unlike other forms of crime, terrorism strives for effect that in turn would provoke a reaction, which significantly lowers the violence threshold that its perpetrators may be ready and willing to pass.

The report discusses the challenges to identifying would-be terrorists and pre-empting terrorist attacks by drawing upon the burgeoning literature on the process of radicalisation. The concept of a hybrid investigation is understood as a two-fold complex of measures that aim to (1) facilitate the early identification of the risk of violent radicalisation and (2) directly support counter-terrorism. In unpacking this concept,

[1] Europol, ***European Union Terrorism Situation and Trend Report 2021 (TESAT)***, Publications Office of the European Union, Luxembourg, 7 December 2021

the report reviews existing strategies and tactics for addressing specific aspects of terror-related activities and the ways in which stakeholders outside law enforcement and security services could contribute to the prevention of violent radicalisation.

Mapping the Phenomenon of Terrorism

This section approaches the phenomenon of terrorism from two perspectives. First, the section looks into the psychology of terrorism focusing on the process of violent radicalisation. Second, the section looks into the criminalisation of terrorism at the EU level.

Psychology of Terrorism and the Process of Violent Radicalisation

The claim that terrorist perpetrators are, by definition, mentally unstable or exhibit signs of psychopathological disorders which makes them prone to violence has a long history in the study of the psychology of terrorism.[1] According to this view, terrorists inherently possess certain abnormal features that make them different from ordinary people. However, overreliance on the idea of a 'terrorist personality' runs the risk of obscuring or diminishing the role that external factors play in shaping one's choice to engage in politically-motivated violence. For example, John Horgan notes that "a theory of terrorist behaviour must accommodate the heterogeneity of the phenomenon as well as the wide diversity of individual motivations that terrorist members might themselves push as explanatory factors. Heterogeneity is a very pervasive emergent theme, across and within movements, and this is a useful reason to study historical and bibliographical accounts of terrorism within psy-

[1] Andrew Silke, **"Cheshire-cat logic: The recurring theme of terrorist abnormality in psychological research"**, *Psychology, Crime, and Law*, vol. 4:1 (1998), pp. 51-69

chological contexts."[2] Andrew Silke has also cautioned against adopting a one-sided view on the issue of terrorist profiling: "In order to understand the psychology of 'terrorists', one must expect considerable variation between the people involved. There is no one path into terrorism. […] Ultimately, it is the combined impact of a number of factors that pushes and pulls someone into becoming a terrorist, and these factors will vary depending on the culture, social context, terrorist group, and individual involved. Becoming a terrorist is for most people a process. It is not usually something that happens quickly, or easily."[3]

When analysing possible motivations for engaging in terrorist activity, Silke has identified several groups of push and pull factors that could help explain why individuals join terrorist groups or movements.[4] For instance, research suggests a positive correlation between certain biological properties such as age and sex, insofar as a significant proportion of terrorist recruits are young (teenagers / early twenties) males. Relative deprivation, marginalisation, and actual or perceived discrimination can shape social identity and the ways in which individuals deal with and resolve grievances. People on the margins are likely to be more susceptible to supporting violent activism if favourably exposed to narratives and ideologies advocating a radical change in the mainstream social system. A desire for vengeance can be a powerful motivating factor to resort to violence. Moreover, personal accounts of terrorist perpetrators suggest that one does not need to experience unjust events first-hand; on the contrary, watching violent events on television or online can create a sense of perceived injustice and make one identify themselves with the victims. As a result, joining a terrorist group is seen as a way of taking action to correct the situation and restore justice. As regards pull factors, membership in terrorist groups can be seen as boosting one's social status and offering personal gains such as improved self-esteem and a degree of protection. On the opposite spectrum of the continuum, individuals may be pressed to join a terrorist group by peers or recruiters.[5]

Borum has suggested a four-stage process of ideological development for assessing the behaviours, experiences, and activities of a group or individual associated with extremist ideas.[6] In this model, the process of extremist ideology formation requires an undesirable condition or event which is considered not right and therefore needs to be corrected. This provides a context. The undesirable circumstances are then framed as unjust, since they do not apply to everyone. Injustice does not occur by itself which leads to attribution and blaming somebody else for one's undesirable circumstances. At the final stage, extremists deem the person or the group responsible for the perceived injustice as bad (as good people do not inflict on others conditions that are not right and fair). According to Borum, this ascription facilitates violence in three ways: (1) aggression becomes more justifiable and acceptable when aimed at 'bad' people, especially those who intentionally cause harm to others; (2) designating somebody as 'bad' allows dehumanisation; and (3) those suffering adverse conditions at the hands of 'bad' people (i.e. extremists) do not perceive themselves as bad (Figure 1).[7]

[2] John Horgan, 'The Search for the Terrorist Personality' in A. Silke (ed.), *Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences*, Wiley, 2003, pp. 3-28. See also John Horgan, **'From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism'**, *Annals of the American Academy of Political and Social Science*, vol. 618 (2008), pp. 80-94

[3] A. Silke, 'Becoming a Terrorist' in A. Silke (ed.), *Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences*, Wiley, 2003, pp. 29-54

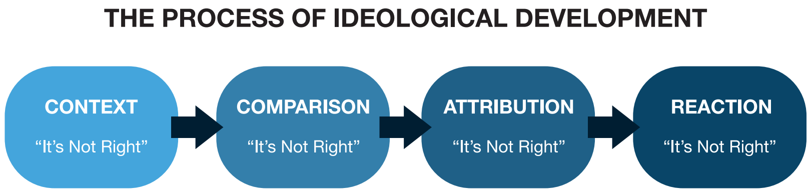
[4] A. Silke, 'Becoming a Terrorist' in A. Silke (ed.), *Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences*, Wiley, 2003, pp. 29-54

[5] A. Silke, 'Becoming a Terrorist' in A. Silke (ed.), *Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences*, Wiley, 2003, pp. 29-54

[6] Randy Borum, **'Understanding the Terrorist Mind-Set'**, *FBI Law Enforcement Bulletin*, vol. 72:7 (2003), pp. 7-10

[7] Randy Borum, **'Understanding the Terrorist Mind-Set'**, *FBI Law Enforcement Bulletin*, vol. 72:7 (2003), pp. 7-10

Figure 1: Four-stage process of ideological development



Based on R. Borum, "Understanding the Terrorist Mind-Set", *FBI Law Enforcement Bulletin*, vol. 72:7 (July 2003)

Borum underlies the importance of considering extremist patterns from the perspective of social cognition. In particular, he notes that "gaining insight as to how someone may resolve a particular dilemma or handle a given situation requires a consideration of the person's entire perspective as influenced not only by their values and beliefs but by other factors, such as the information they have been exposed to, their assumptions, and their life experiences – in short, how they view the world. All people operate on their own internal 'map' of reality, not reality itself."[8] He also cautions against overemphasising the role of ideology as the sole motive for committing a terrorist offence. Some individuals, for example, may be predisposed to aggressive behaviour or criminality and simply use a particular cause or ideology to justify their acts. And even those who believe in the ideology may engage in violence as a result of a combination of factors.[9]

[8] Randy Borum, **'Understanding the Terrorist Mind-Set'**, *FBI Law Enforcement Bulletin*, vol. 72:7 (2003), pp. 7-10

[9] Randy Borum, **'Understanding the Terrorist Mind-Set'**, *FBI Law Enforcement Bulletin*, vol. 72:7 (2003), pp. 7-10

Some commentators rely on terror management theory (TMT) to account for violent extremism and the psychological, cultural, social and historical forces that lead people to support terrorist aggression.[10] TMT holds that humans possess an innate propensity to imbue life with meaning as a way of coping with death salience, i.e. unlike other beings, people are aware of the fact that death is inevitable which can create paralysing anxiety and mental turmoil. Adherence to socially constructed worldviews (or in Geertz's language, 'web of significance') allow humans to develop a sense of value and self-esteem: "Being a valuable contributor to a meaningful reality makes it possible to transcend death either literally, by being granted entrance into an eternal paradise (e.g. heaven, nirvana), or symbolically, through societal remembrance in the form of memorial statues, awards or other lasting markers of our existence."[11] This in turn has implications for the formation of a group identity: "Because cultural worldviews and self-esteem are both sets of humanly created ideas, and there is no way of knowing if they are correct in any absolute sense, faith in them depends on social consensus from others. Those who share one's worldview and view one in a positive light increase faith in one's worldview and bolster self-esteem, thus increasing the effectiveness of both in managing anxiety; those with different worldviews and who view one in a negative light threaten faith in one's worldview and self-esteem, thus undermining their effectiveness in managing anxiety. […] TMT suggests that this dynamic predisposes people to be loyal to their group, society and culture and to be hostile toward those with different affiliations."[12] Pyszczynski et al. note that the idea that cultural worldviews are fragile social constructions that must be continually consensually validated in order for them to maintain their

[10] Tom Pyszczynski et al. **'Righteous Violence: Killing for God, Country, Freedom and Justice'**, *Behavioural Sciences of Terrorism and Political Aggression*, vol. 1:1 (2009), pp. 12-39

[11] Tom Pyszczynski et al. **'Righteous Violence: Killing for God, Country, Freedom and Justice'**, *Behavioural Sciences of Terrorism and Political Aggression*, vol. 1:1 (2009), pp. 12-39. See also Clifford Geertz, *The Interpretation of Cultures*, Basic Books, 1973

[12] Tom Pyszczynski et al. **'Righteous Violence: Killing for God, Country, Freedom and Justice'**, *Behavioural Sciences of Terrorism and Political Aggression*, vol. 1:1 (2009), pp. 12-39

effectiveness as anxiety buffers is of particular relevance to the terror management perspective on terrorism. Support for violence and hostility toward those who are different or threaten one's worldview stems from a deeply rooted existential fear from which cultural worldviews function as a safety net. One of the side effects of the use of violent tactics is that thoughts of death are constantly re-activated, leading to greater need for the protection provided by one's worldview, which leads to greater support for hostilities against those who threaten them, leading to an ongoing cycle of escalating violence.[13]

Whilst TMT offers insights into the causes of violent resolution of inter-group conflicts, it does not fully account for the distinction between passive supporters of terrorism (i.e. individuals who may share the goals of terrorist groups but do not engage in violence) and active terrorist operatives. On the contrary, it suggests that there are additional factors that impact on one's decision to turn to violent extremism. Over the past two decades, the issue of radicalisation has received considerable attention both in academic and policy circles.[14] Box 1 provides indicative definitions of the terms 'radicalisation', 'extremism', and 'violent extremism', in order to compare and contrast these concepts.

[13] Tom Pyszczynski et al. **'Righteous Violence: Killing for God, Country, Freedom and Justice'**, *Behavioural Sciences of Terrorism and Political Aggression*, vol. 1:1 (2009), pp. 12-39

[14] EUCPN, ***European Crime Prevention Monitor 2019/ 1: Radicalisation and Violent Extremism***. Brussels: European Crime Prevention Network, 2019

Box 1: Defining radicalisation and extremism

Radicalisation

The process of social, psychological, and ideological changes leading to extremism and potentially violent extremism.

Extremism

An ideological position characterised by a polarised world-view, a distrust in state institutions and democratic decision-making processes, and the legitimation of the use of violence.

Violent extremism

The position of an individual who actually has committed one or more acts of violence out of extremist considerations.

Source: EUCPN, ***European Crime Prevention Monitor 2019/ 1: Radicalisation and Violent Extremism***. Brussels: European Crime Prevention Network, 2019.

Radicalisation of attitudes does not necessarily result into radicalisation of behaviour which has given rise to a conceptual fault line between the notions of radicalisation that emphasise extremist beliefs ('cognitive radicalisation') and those that focus on extremist behaviour ('behavioural radicalisation').[15] This conceptual fault-line has driven the scholarly debate on but it has also provided a backdrop for distinguishingly different policy approaches for dealing with extremism. Neumann identifies two broad categories of approaches for countering radicalisation: an 'Anglo-Saxon' approach and a 'European' approach.[16] Whereas the Anglo-Saxon approach aims to address behavioural radicalisation, especially acts of terrorism and violence, the European approach aims to confront cognitive and behavioural radicalisation placing a greater emphasis on the former. The European approach is also consistent with the

[15] Peter Neumann, **'The Trouble with Radicalisation'**, *International Affairs*, vol. 89:4 (2013), pp. 873:893

[16] Peter Neumann, **'The Trouble with Radicalisation'**, *International Affairs*, vol. 89:4 (2013), pp. 873:893

idea that radicalisation is a process, whereby individuals 'move' from a state of cognitive to behavioural radicalisation. For example, some commentators discuss different components of radicalisation such as cognitive, affective, and behavioural.[17] At the cognitive level, radicalisation involves two features: (1) knowledge of alternative moral systems that support terrorism; and (2) the incorporation of an alternative morality as integral to one's identity (i.e. coming to perceive oneself as a person who legitimately condones terrorism). At the affective level, radicalisation involves undergoing social learning that prepares an individual to take terrorist action. Such learning processes focus on sidestepping the inhibitory mechanisms that prevent humans from injuring or killing, and also have to be sidestepped in military training. And at the behavioural level, radicalisation involves engaging in acts of violence.[18]

The process of violent radicalisation can be approached in terms of phases. Doosje et al. have suggested an individual follows three phases during the radicalisation process: (1) a sensitivity phase, (2) a group membership phase, and (3) an action phase.[19] Each phase is conditioned by factors at the *micro*, i.e. individual, *meso*, i.e. group, and *macro*, i.e. social.[20] Micro-level factors that come into play at the sensitivity phase may include a desire to improve one's self-esteem, assert one's significance, and overcome personal uncertainty by turning to an ideology for meaning and structure in life.[21] Meso-level factors at this phase may include the impact of family environment, perceived discrimination and use of double standards, and social circle, including friends and peer pressure. Macro-level factors here may include broader societal factors such as the impact of globalisation on one's lifestyle and culture. During the sensitivity phase, individuals experience what is known as 'cognitive opening', usually as a result of a personal crisis or encounter with some persistent undesirable circumstances, which makes them more responsive to new ideas and alternative explanations of reality.[22]

At the group membership phase, an individual who is already experiencing a cognitive opening, joins a radical group.[23] Motivation to demonstrate one's loyalty to the group could serve as a powerful micro-level factor for radicalisation at this phase and, eventually lead to a state whereby the individual start downgrading the out-group in public contexts. This in turn fuels and feeds into a meso-level factor related to solidifying the bonds between the individual and other group members. The culmination of this process of bond formation entails the breaking of relations with family and friends. Macro-level factors at this phase concern the relationship between the radical group and the rest of society. For example, the stronger the perception of the success or efficacy of the radical group, the higher its social standing and the greater the likelihood of attracting new recruits and expanding the pursued agenda.

At the action phase, radicalised individuals engage in violence.[24] The desire for revenge for the death of a close one could be an important micro-level factor here. Meso-level factors at this phase may include demanded commitment to perpetrating acts of violence and de-humanisation of the out-group. A key macro-level factor at this phase could be the belief that violence is the only possible way of realising the radical group's demands.

[17] Fathali Moghaddam, 'De-radicalisation and the Staircase from Terrorism' in D. Canter (ed.) *The Faces of Terrorism: Multidisciplinary Perspectives*, Wiley, 2009 pp. 277-292

[18] Fathali Moghaddam, 'De-radicalisation and the Staircase from Terrorism' in D. Canter (ed.) *The Faces of Terrorism: Multidisciplinary Perspectives*, Wiley, 2009 pp. 277-292

[19] Bertjan Doosje et al. **'Terrorism, Radicalisation, and De-Radicalisation'**, *Current Opinion in Psychology*, vol. 11 (2016), pp. 79-84

[20] See Alex Schmid, ***'Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review'***, The International Centre for Counter-Terrorism – The Hague 4, no. 2, 2013

[21] Bertjan Doosje et al. **'Terrorism, Radicalisation, and De-Radicalisation'**, *Current Opinion in Psychology*, vol. 11 (2016), pp. 79-84

[22] Simona Trip et al., **'Psychological Mechanisms Involved in Radicalization and Extremism. A Rational Emotive Behavioral Conceptualization'**, *Frontiers in Psychology*, 6 March 2019

[23] Bertjan Doosje et al. **'Terrorism, Radicalisation, and De-Radicalisation'**, *Current Opinion in Psychology*, vol. 11 (2016), pp. 79-84

[24] Bertjan Doosje et al. **'Terrorism, Radicalisation, and De-Radicalisation'**, *Current Opinion in Psychology*, vol. 11 (2016), pp. 79-84

Terrorist Offences and Offences Related to Terrorist Activities

Groups, organisations, and networks of different ideological, political, or religious stripe have used terrorism as a tactic. Terrorist activities are wide-ranging and it is not uncommon for terrorist groups to make use of advances in science and technology in pursuing their agendas. Access to weaponry, including explosives and unconventional warfare materials, such as chemical, biological radiological or nuclear substances can influence the course of planning and carrying out terrorist attacks. Information and communication technologies (ICTs) feature increasingly in the activities of radical groups, particularly as regards the dissemination and exchange of extremist content; the recruitment of new members; and the plotting acts of violence. Sources of terrorism financing can vary significantly ranging from legal and illegal funds to the abuse of charities or even self-funding.[25] Some forms of cyber-crime have also been deployed for diverting or raising funds to support violent extremism. Whilst there is little evidence of systematic cooperation between criminals and terrorists, some overlap between organised crime groups and extremist groups has been observed, for example, as regards weapon procurement and drug trafficking.[26]

EU Directive 2017/541 on combatting terrorism lists illicit activities (e.g. attacks upon person's life and/or physical integrity; kidnapping or hostage-taking; seizure of means of public or goods transport; arson; procurement and use of explosives, fire arms, or other types and forms of weaponry; destruction or disruption of critical infrastructure and other essential public services) that need to be defined as terrorist offences under national legislation when committed for the following purposes:

[25] Europol, ***European Union Terrorism Situation and Trend Report 2021 (TESAT)***, Publications Office of the European Union, Luxembourg, 7 December 2021

[26] Europol, ***European Union Terrorism Situation and Trend Report 2021 (TESAT)***, Publications Office of the European Union, Luxembourg, 7 December 2021

- To seriously intimidate a population
- To unduly compel a government or an international organisation to perform or abstain from performing any act
- To seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation[27]

This Directive further defines criminal offences that relate to directing a terrorist group or participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, knowing that such participation will contribute to the criminal activities of the terrorist group. Offences related to terrorist activities include public provocation to commit an act of terrorism; recruitment for terrorism; providing or receiving training for terrorism, including instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances; travelling for the purpose of terrorism or otherwise organising or facilitating such travelling; terrorist financing; aggravated theft, extortion, or drawing up or using false administrative documents with a view to committing a terrorist offence.[28] Aiding and abetting, inciting and attempting terrorist offences is also punishable.

Whilst Directive 2017/541 is primarily a criminal law instrument, some of its provisions appear to envisage that Member States can put in place measures outside the scope of criminal law, such as those related to public provocation content online (Art. 21) or non-criminal sanctions for legal persons (Art. 18).[29] This assumption is not unfounded, since

[27] **Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA**

[28] **Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA**

[29] European Union Agency for Fundamental Rights, ***Directive (EU) 2017/541 on combating terrorism – Impact on Fundamental Rights and Freedoms***, 18 November 2021

Art. 28 (1) lists regulations and administrative provisions, in addition to laws, among the means of transposition. The results of a recent study published by the European Union Agency for Fundamental Rights (FRA) indicate that in some Member States, the introduction of administrative measures accompanies the criminalisation of terrorist offences that the Directive covers, including in relation to travel, training and public provocation. Some of these measures are applied as a consequence of criminal convictions for offences that the Directive requires Member States to criminalise, such as post-sentence monitoring and movement restriction measures or deprivation of nationality. Others are used in a direct connection with the detection and investigation of such offences, in a preventive manner against persons suspected of radicalisation and of planning to commit an offence such as travelling for the purpose of terrorism. Still others may have an impact on how Member States apply EU law in other fields, such as border management and returning illegally staying non-EU nationals when measures are taken on security grounds in the context of immigration legislation.[30]

A common challenge that countries face when dealing with terrorism is the process of balancing fundamental rights considerations with national security concerns. Appropriate oversight and guarantees for the procedural rights of those suspected or accused of terrorist activities, including by means of judicial review are essential for ensuring that counter-terrorism approaches are in line with existing human rights standards.

[30] European Union Agency for Fundamental Rights, ***Directive (EU) 2017/541 on combating terrorism – Impact on Fundamental Rights and Freedoms***, 18 November 2021

Mapping the Phenomenon of Terrorism

This section focuses on the process of collecting data for preventing and pre-empting terrorist attacks. This includes identifying would-be terrorist perpetrators. Given the clandestine nature of terrorist activities, gathering reliable intelligence is pervaded with challenges. The concept of hybrid investigations is used here to denote two complementary lines of effort, namely measures that aim to (1) facilitate the early identification of the risk of violent radicalisation and measures that (2) directly support counter-terrorism. To unpack this concept, existing strategies and tactics for addressing specific aspects of terror-related activities and the ways in which stakeholders outside law enforcement and security services could contribute to the prevention of violent radicalisation are reviewed.

Preventing Terrorist Offences: The Role of Policing

Modern police service is based on the principle of prevention.[1] Crime prevention is an essential part of proactive policing, community policing, proximity policing and all their variants. The main purpose and goal of intelligence-led policing also is prevention. In broad terms, prevention and preventive measures are aimed at preventing situational and direct causes and reasons of the problems of security, liveability, and criminality and limiting their consequences.[2]

[1] Sirpa Virta, **'Future Preventive Policing'**, *European Police Science and Research Bulletin*, No.2 (2017), pp. 135-141

[2] Sirpa Virta, '**Future Preventive Policing'**, *European Police Science and Research Bulletin*,

The general framework of crime prevention is relevant to counter-terrorism. The European Urban Charter adopted in 1992 sets out a body of principles on urban management that focus on safety and crime prevention. These principles include as follows:

1. A coherent safety and crime prevention policy must be based on prevention, law enforcement, and mutual support.
2. A local safety policy must be based on up-to-date comprehensive statistics and information.
3. Crime prevention involves every member of the community.
4. An effective urban Safety policy depends on close co-operation between the police and the local community.
5. A local anti-drug policy must be defined and applied.
6. Programmes for preventing relapse and developing alternatives to incarceration are essential.
7. Support for victims is a key component of any local urban Safety policy.[3]

Through the perspective of prevention, crime is considered a security risk.[4] Crime prevention is thus underpinned by several inter-related trends (Box 2).

No.2 (2017), pp. 135-141

[3] European Forum, ***SECUCITIES: Urban Crime Prevention Policies in Europe: towards a common culture?***, 2004

[4] Sirpa Virta, **'Future Preventive Policing'**, *European Police Science and Research Bulletin*, No.2 (2017), pp. 135-141

Box 2: Trends in Crime Prevention

Importance of knowledge-based prevention

The regular evaluation of prevention programmes is key to developing policies that are based on reliable data, including data collected and analysed by independent authorities.

Significant efforts have been undertaken to track the evolution of crime in terms of standardising, matching, and comparing data. Despite the absence of shared definitions for offences, the development of "international standards" helps to overcome some of the cultural and legal differences in measuring certain types of crime. An increasing number of international exchange networks s are dedicated to observing and analysing crime trends and prevention approaches, or developing evaluation methodologies. They are important platforms for the dissemination and adaptation of good strategies in terms of their transferability between different contexts.

Unequal involvement of public authorities in prevention

The role of police is not clearly defined but they continue to be perceived the dominant actors in prevention. The criminal justice system is less obviously concerned with prevention, even though its formal role is recognised. Legal interventions tend to privilege conflict management and dialogue between actors and victims of crime and forms of restorative justice are increasingly being favoured.

The criminalisation of behaviours generally responds to a strictly criminal justice approach to community safety. There are increasing penalties for violence against women and disciplinary school problems and specific offences have been created to draw attention to these and other problems. Marginalisation is also increasingly treated as a 'nuisance" that needs to be managed. Yet increased regulations multiply the possibilities for breaking the law and contradict international standards and norms that privilege a more social and educational approach to deviant behaviour and crime based on their causes, and which advocate more nuanced and diversified responses.

A need for 'new' community support services

Innovative approaches to crime prevention help increase safety and a sense of security either through supporting institutions traditionally assigned with this task (e.g. the police) or by providing additional social support and mediation services. Such approaches aim to improve services to the population by being more available locally, increasing human presence in the evenings and at night, and promoting understanding and dialogue with authorities.

The development of integrated approaches to prevention appears limited, in part because such approaches entail a method rather than a model. Integrated prevention delivers results in terms of improving community safety and reinforcing the capacities of local actors. It mobilises communities and favours collective development. Yet the implementation of integrated prevention requires tested tools privileging audits, partnerships, and a multidisciplinary analysis of crime. Safety audit tools are enhanced by victimisation surveys, observatories, and innovative participatory tools such as exploratory walks, and by technology such as geocoding. Evaluation approaches have diversified, and include more pragmatic action-research methods, and process evaluations.

Reinforcing the role of local actors in prevention

Crime prevention is essential to sustainable development, as is the prevention of problems linked to poverty, health, education, and urban development. Vibrant communities are not possible without safety and social cohesion. Crime prevention involves not only the search for a permanent balance between approaches and actions privileged at different government levels, but also takes account of the specific characteristics of each particular context.

Local authorities and community actors including the private sector are best placed to identify the needs and potential of the local population. Whilst their role in crime prevention is more frequently recognised, their legal status and financial resources are still largely limited.

Source: Julie Bodson et al., ***Crime Prevention and Community Safety: Trends and Perspectives***, International Centre for the Prevention of Crime, June 2008.

There are different approaches to crime prevention.[5] Primary crime prevention includes universal approaches that aim to prevent crime before it occurs. Secondary crime prevention includes approaches that focus on those people who are at the highest risk of victimisation and perpetration of violence. And tertiary crime prevention includes approaches that focus on people who have already been victimised or violent. Complementary approaches that can be applied at different stages of crime prevention include:

- Situational crime prevention – this refers to the reduction of crime through the management, design, and augmentation of the physical environment. Indicative measures include the installation of surveillance cameras in public spaces and controlling access to buildings.
- Social crime prevention – this refers to supporting individuals and communities through social, economic, health, and educational measures. The aim is to strengthen community bonds, increase levels of informal social control and thus deter actual or potential offenders.
- Prevention of recidivism – supporting the reintegration of offenders.[6]

[5] European Forum, ***SECUCITIES: Urban Crime Prevention Policies in Europe: towards a common culture?***, 2004

[6] European Forum, ***SECUCITIES: Urban Crime Prevention Policies in Europe: towards a common culture?***, 2004

When it comes to terrorism prevention, law enforcement agencies and other local authorities face a dual challenge.[7] On the one hand, there is a need for relevant expertise to confront the risks of modern terrorism. One the other hand, the diversity of preventive actions requires excellent coordination between all agents involved, be they in the same organisation (horizontal cooperation), or at other levels of the state or with foreign partners (vertical cooperation). Policing, especially preventive policing and community policing are considered vital tools for counter-terrorism.[8] Virta notes that "intelligence-led policing, and intelligence, have become an additional element to the field of preventive policing. […] Intelligence and intelligence-management processes (intelligence gathering, strategic analysis, targeting and exchange) improve the capacity of community policing and other preventive policing initiatives."[9] He further comments that "radicalisation is a challenge for preventive policing. When trying to prevent radicalisation which may lead to (home-grown) terrorism the police have to assess local community context and tensions and the state of the society, and keep in mind national security threat assessments and priorities, as well as European and global terrorism threat assessments. Intelligence requirements are potentially endless."[10] Within this context, commentators highlight the role of civic education for law enforcement and policing personnel in strengthening capacities for preventing violent extremism and promoting democracy and fundamental rights.[11]

[7] European Forum, ***SECUCITIES: Cities Against Terrorism – Training Local Representatives in Facing Terrorism***, 2007

[8] Sirpa Virta, **'Future Preventive Policing'**, *European Police Science and Research Bulletin*, No.2 (2017), pp. 135-141

[9] Sirpa Virta, **'Future Preventive Policing'**, *European Police Science and Research Bulletin*, No.2 (2017), pp. 135-141

[10] Sirpa Virta, **'Future Preventive Policing'**, *European Police Science and Research Bulletin*, No.2 (2017), pp. 135-141

[11] Andreas Pudlat and Patricia Schütte-Bestek, **'Preventing Violent Extremism and Strengthening Democracy – Civic Education in Law Enforcement and Policing in Germany'**, *Euro-*

Countering radicalisation in cyberspace

The 2018 edition of the Europol report, Internet Organised Crime Threat Assessment (IOCTA) draws attention to the ways in which the Islamic State used the internet to spread its propaganda and inspire acts of terrorism.[12] The report notes that takedown efforts by law enforcement agencies pushed ISIS supporters into using encrypted messaging apps which offer private and closed chat groups, the dark web, or other platforms which are less able or willing to disrupt their activity. ISIS specifically targeted individuals with skills in information and communication technologies who shared instructional videos offering tips about encryption and discussing the surveillance capabilities of hostile governments. Other tutorials included advice on how to sign up to Twitter or Facebook without having to register a mobile phone number and how to deactivate GPS tagging when taking or posting a photo. The report further notes that while IS cybercrime capability remained limited at the time, the technologically advanced use of encrypted communication tools for disseminating propaganda allowed the group to attract supporters tapping wide-ranging human expertise.[13]

A study published by UNESCO in 2017 on the impact of violent extremism available in social media on youth also suggests that social media can facilitate violent radicalisation through the dissemination of information and propaganda, as well as the reinforcement, identification and engagement of a (self)-selected audience that is interested in radical and violent messages."[14]

The use of the internet for sharing extremist content and recruiting terrorist operatives precedes the active years of ISIS. Examples that online terrorist activity commonly focuses on communication, propaganda, research, planning, publicity, fundraising, and creating a distributed sense of community date back to 2006.[15] Brown and Koff note: "Terrorist websites make strong efforts to increase public sympathy for their cause and sow doubts about the validity of the status quo. The Internet is an ideal propaganda tool and most extremist groups therefore have a Web presence. Sites are cheap to produce while looking professional, adding validity and legitimacy to a cause. It is relatively easy for extremists to use multimedia, which appeals to the young and less literate. […] Groups can now bypass [press coverage] gatekeepers and communicate directly with supporters and potential recruits. […] Sites are also a route for disinformation and psychological operations such as casualty figures and attack warnings."[16] The authors further observe that: "The Internet has also changed the way global terrorism functions. Groups can now be more geographically dispersed and non-hierarchical. Such networks have been proven capable of defeating much more powerful hierarchies. 'Leaderless resistance', which originated in printed media, can now work much more effectively. Terrorist organisations can flourish without state sponsors, who are vulnerable to threats of retaliation. They are instead sponsored by sub-state entities that operate more like corporations." This claim is balanced by asserting that: "Terrorist use of new technologies provides new opportunities for intelligence gathering and disruption of operations by intelligence agencies. They can use active and passive attacks (using viruses and surveillance/traffic analysis) on terrorist computers to gather address books, cookies, passwords and similar information. Counter-terrorist operations include the use of black propaganda to destroy trust. If agencies can identify and take out purveyors of good technical information, they can flood channels with misinformation and leave the less informed to propagate bad information. At the same time they gather intelligence on participants, organisations and their modus operandi. Most ideological debate takes place on open

pean Police Science and Research Bulletin, No.3 (2017), pp. 245-249

[12] Europol, ***Internet Organised Crime Threat Assessment 2018 – IOCTA***, 18 September 2018

[13] Europol, ***Internet Organised Crime Threat Assessment 2018 – IOCTA***, 18 September 2018

[14] Seraphin Alava et al., ***Youth and Violent Extremism on Social Media: Mapping the Research***, UNESCO, 2017

[15] Ian Brown and Douwe Korff, **'Terrorism and the Proportionality of Internet Surveillance'**, *European Journal of Criminology*, vol. 6:2 (2009), pp. 119-134

[16] Ian Brown and Douwe Korff, **'Terrorism and the Proportionality of Internet Surveillance'**, *European Journal of Criminology*, vol. 6:2 (2009), pp. 119-134

recognised sites, including from senior participants, which allows up-and-coming leaders to be identified."[17]

Extensive research has been carried out to support the identification of extremist narratives online and detect radicalisation on social networks.[18] Based on research on jihadist radicalisation, Denaux and Gomez-Perez have put forward an indicative taxonomy to comprising three categories of narratives: (1) cultural; (2) strategic; and (3) individual or local narratives.[19] Saif et al. have used semantic graph-based approach to identify pro-ISIS and anti-ISIS messaging to detect radicalisation signals on Twitter.[20] The social media research carried out by Rowe and Saif aims to offer insights into three inter-related issues: (1) detecting pro-ISIS stance on social media; (2) detecting behaviour divergence toward radicalisation; and (3) factors influencing the adoption of pro-ISIS language online.[21] Their work suggests that social dynamics play a strong role in term uptake where users are more likely to adopt pro-ISIS language from users with whom they share many interacted users (either via having communicated with those users beforehand, or shared content from them). The authors also note that prior to being activated and rejecting their previous behaviour, users go through a period of significant increase in adopting innovations (i.e. communicating with new users and adopting new terms).[22] To counter the increasing spread of extremist content online, in 2016 UNESCO published a comprehensive study on policy options and regulatory mechanisms for managing radicalisation on the Internet.[23] This study offers insights into the extent to which the online space can and should be regulated and the role that private sector service providers can play in the prevention of radicalisation risks. It also lists possible strategies for filtering extremist content, blocking suspicious websites, as well as encryption and use of counter-narratives.

Commentators suggest that it is possible track and trace online behaviours on social media to proactively identify potential violent terrorist attackers.[24] Aly notes that "there are certain markers – thematic, emotional and behavioural – that can be used to build a more comprehensive profile of a potential suspect. They are detectable on the average user's social media profile. Thematic markers include allegiance to radical groups or figures, in-group ideology and pride, out-group derogation, and identification as a 'soldier' or 'warrior', as expressed through symbols, likes, associations, images and subscriptions. Key emotional markers are anger and contempt for and disgust at the out-group. Behavioural markers include fixation (an increasingly pathological preoccupation with a person or cause); identification (a desire to be or identify as an agent for a cause); and leakage (the communication of the intent to carry out violence)."[25] She outlines an indicative framework for mapping terrorist behaviour online (Box 3).

[17] Ian Brown and Douwe Korff, **'Terrorism and the Proportionality of Internet Surveillance'**, *European Journal of Criminology*, vol. 6:2 (2009), pp. 119-134

[18] See, for example, Raúl Lara-Cabrera et al. **'Measuring the Radicalisation Risk in Social Networks'**, *IEEE Access*, vol. 5 (2017), pp. 10892 – 10900

[19] Ronald Denaux and Jose Manuel Gomez-Perez, ***Textual Analysis for Radicalisation Narratives aligned with Social Sciences Perspectives***, CEUR Workshop, 14 April 2019

[20] Saih, H et al. ***A Semantic Graph-Based Approach for Radicalisation Detection on Social Media,*** ESWC 2017: The Semantic Web – Proceedings, Part I, Lecture Notes in Computer Science, Springer, 2017, pp. 571–587

[21] Matthew Rowe and Hassan Saif, ***Mining Pro-ISIS Radicalisation Signals from Social Media Users***, Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016) pp. 329–338

[22] Matthew Rowe and Hassan Saif, ***Mining Pro-ISIS Radicalisation Signals from Social Media Users***, Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016) pp. 329–338

[23] UNESCO, ***Policy Options and Regulatory Mechanisms for Managing Radicalization on the Internet***, 30 September 2016

[24] Anne Aly, **'An Evolution of Terrorism: the intersection of cybercrime and terrorist activity'** in Leanne Close and Daria Impiombato (eds.), *Counterterrorism Yearbook 2021*, ASPI, 31 March 2021

[25] Anne Aly, **'An Evolution of Terrorism: the intersection of cybercrime and terrorist activity'** in Leanne Close and Daria Impiombato (eds.), *Counterterrorism Yearbook 2021*, ASPI, 31 March 2021

Box 3: Behavioural indicators for terrorist activity online

The **seeker** is primarily motivated to acquire any information about an extremist ideology or idea and is likely to be cognitively open to receiving new information.

The **lurker** has already narrowed their information sources and has started to rigidify their mindset around extremism, while their social media associations start to gravitate towards ideological themes.

The **inquirer** uses political aggression in their posts as they begin making connections between a perceived obstruction to their own life goals and the actions of their out-group. Their likes and associations may be skewing towards certain extremist or extremist-sympathising pages.

The **advocate** adopts a confrontational and declarative posting style. Their profile and cover photos contain symbols associated with an extremist ideology, images associated with conflict, or both. Their likes and associations overtly support an ideology.

The **activator** is either activating, or about to activate, their extremist ideologies offline in the commission of a violent extremist act.

Source: Anne Aly, ***'An Evolution of Terrorism: the intersection of cybercrime and terrorist activity'*** in Leanne Close and Daria Impiombato (eds.), *Counterterrorism Yearbook 2021*, ASPI, 31 March 2021.

The role of social media intelligence (SOCMINT) in identifying criminal activity, giving early warning of disorder and threats to the public, or building situational awareness in rapidly changing situations has been discussed with relation to addressing public safety concerns.[26] Appropriate procedures for the collection and management of SOCMINT are key to ensuring that fundamental rights considerations are addressed. Indicative guiding principles in this regard include as follows:

- principle 1: there must be sufficient, sustainable cause
- principle 2: there must be integrity of motive
- principle 3: the methods used must be proportionate and necessary
- principle 4: there must be right authority, validated by external oversight
- principle 5: recourse to secret intelligence must be a last resort if more open sources can be used
- principle 6: there must be reasonable prospect of success.[27]

Tackling terrorism financing

Terrorism financing is a multi-faceted challenge. Given the clandestine nature of terrorist networks and groups, curbing the flow of resources requires a coordinated effort on several fronts. Schneider and Caruso have reviewed different sources of terrorist financing and offered a typology of existing trends.[28] They note that not all financing comes from illegal activities and that completely legal activities by charities, diaspora, or private companies could also be used to channel funding to terrorist organisations. States and corporate donors comprise another significant source of resources and in some cases legitimate business activities may be used to cover up funding diversion. The phenomenon of misused humanitarianism, whereby charities have been used to disguise terrorist financing merits attention.[29] For example, making donations is considered both a moral and social duty in some cultures and such practices can be abused. Illicit activities, including drug trafficking, trade in counterfeit products, oil smuggling, arms and diamonds trafficking, and money laundering can be used to provide funding to terrorist organisations.[30] One additional tactic commonly used by ISIS

[26] David Omand et al. ***#Intelligence***, Demos, 2012

[27] David Omand et al. ***#Intelligence***, Demos, 2012

[28] Friedrich Schneider and Raul Caruso, ***The (Hidden) Financial Flows of Terrorist and Transnational Crime Organizations: A Literature Review and Some Preliminary Empirical Results***, Economics of Security Working Paper 52, 2011

[29] Liam McGee, ***Preventing and Combating the Financing of Terrorism***, Issue Brief, Old Dominion University, 2020

[30] Friedrich Schneider and Raul Caruso, ***The (Hidden) Financial Flows of Terrorist and Transnational Crime Organizations: A Literature Review and Some Preliminary Empirical Results***, Economics of Security Working Paper 52, 2011

was kidnapping for ransom.[31]

Banking and money transferring practices have been misused to facilitate the flow of funding for criminal activities, including through money laundering. A case in point is the informal money transfer system, Hawala. Commentators have described this system as follows: "Hawala bankers are financial service providers who carry out financial transactions without a license and therefore without government control. They accept cash, cheques or other valuable goods (diamonds, gold) at one location and pay a corresponding sum in cash or other remuneration at another location. Unlike official banks, Hawala bankers disregard the obligations concerning the identification of clients, record keeping, and the disclosure of unusual transactions, to which these official financial institutions are subject. Through the Hawala system that forms an integral part of the informal black market economy, underground bankers ensure the transfer of money without having to move it physically or electronically. When a payment needs to be made overseas, the underground banker will get in touch with a courier (or more recently using email, fax or phone) in that country informing him of the details of making the payment. If the recipient of the payment wishes to personally obtain the money, a code referring to the underground banker in the country of payment is given to the recipient. Such a system is almost untraceable since it leaves little if any paper trail. Transaction records are, if they are kept at all, being kept only until the money is delivered, at which time they are destroyed. Even when there is a paper or electronic record of sorts it is often in dialects and languages that serve as de facto encryption system."[32]

As cybercrime continues to proliferate, so do the opportunities for terrorist financing. A 2021 report by Europol notes that: "The crime-as-a-service (CaaS) model remains a prominent feature of the cybercriminal underground and is a cross-cutting factor throughout the cybercrime sub-areas. The availability of exploit kits and other services not only serves criminals with low technical skills, but also makes the operations of mature and organised threat actors more efficient. […] Legitimate tools and techniques that are abused by cybercriminals include cryptocurrencies and VPNs. Cybercriminals obfuscate and launder illicitly earned funds via cryptocurrencies."[33] When assessing the merging of illicit activities with cybercrime, commentators note the creation of online criminal hubs which can serve as hidden online marketplaces where the trade of traditional illegal goods and services coexists in the "darknet" with the supply of tools to commit cybercrimes.[34] Against this backdrop, identifying suspicious transactions or business and financial operations becomes increasingly challenging which in turn requires the adoption of innovative approaches for tracking illicit financial flows: "The notion of illicit flows aims to connect seemingly disparate illegal activities under a single umbrella to tackle the whole lifecycle of illicit finance – from earning to utilisation – and provide a holistic picture of the issue. The umbrella approach makes even more sense in the digital age, where technology has increasingly become a common enabler. It also makes it possible to adopt harmonised frameworks to trace illegal money, to share best practices between regulatory domains, and, ultimately, to connect previously fragmented efforts."[35]

The Financial Action Task Force (FATF), an inter-governmental standard-setting body which serves as a global money laundering and terrorist financing watchdog has analysed the financing of ISIS noting that the terrorist organisation relied "on grass-root funding sources and utilised efficient delivery mechanisms to obtain funds through the latest tech-

[31] Liam McGee, ***Preventing and Combating the Financing of Terrorism***, Issue Brief, Old Dominion University, 2020

[32] Friedrich Schneider and Raul Caruso, ***The (Hidden) Financial Flows of Terrorist and Transnational Crime Organizations: A Literature Review and Some Preliminary Empirical Results***, Economics of Security Working Paper 52, 2011

[33] Europol, **Internet Organised Crime Threat Assessment (IOCTA) 2021**, 11 November 2021

[34] Tatiana Tropina, **'Big Data: Tackling Illicit Financial Flows'**, in Els De Busser et al. (eds.), *Big Data: A Twenty-First Century Arms Race*, Atlantic Council, 1 June 2017

[35] Tatiana Tropina, **'Big Data: Tackling Illicit Financial Flows'**, in Els De Busser et al. (eds.), *Big Data: A Twenty-First Century Arms Race*, Atlantic Council, 1 June 2017

nology."[36] The report also noted that terrorist fundraising through modern communication networks and the use of crowdfunding techniques have significantly increased over the past decade and highlighted the need for keeping efforts to combat it stay up-to-date. The results of the study show that while a number of traditional countermeasures used to deprive terrorist organisations of their funds were not applicable with respect to the model adopted by ISIS, the organisation's financial, logistical and supply networks remained vulnerable. For example, disruption of command, control and economic structures could hinder ISIS's ability to finance its operations and support its fighters.[37]

A recent report by the FATF reviews the application of new technologies for anti-money laundering (AML) and counter-terrorism financing (CTF) (Box 4). A 2018 study for the Special Committee on Terrorism (TERR) of the European Parliament explores the terrorist financing risks of virtual currencies including cryptocurrencies to provide recommendations for EU policymakers and other relevant stakeholders for ensuring that possible risks are adequately mitigated.[38] The study recommendations read as follows:

- **Ensuring effective, robust, and comprehensive regulation**. Because virtual currencies are rapidly-evolving, borderless technologies that pose a range of complex risks, it is essential that the EU maintain a regulatory framework that is implemented effectively now and remains relevant into the future. Member States should support their local regulatory frameworks with comprehensive legal arrangements designed to prevent and disrupt illicit activity in virtual currencies. This should include ensuring that local law enables the confiscation of virtual currencies during criminal investigations. Policymakers at the national and EU level should take steps to prevent de-risking of the virtual currency industry, which can both hinder innovation and exacerbate risks. Regulators across the EU should provide banks and other financial institutions with clarity about the regulatory status of virtual currency industry participants, and should clarify that the purpose of regulation is to enable the responsible development of the sector.

- **Developing law enforcement knowledge and capacity**. Virtual currencies are complex technologies that require the development of new law enforcement techniques, knowledge and resources. Illicit actors can adapt to these technologies faster than law enforcement can adjust. Member States should expand and accelerate efforts to ensure law enforcement agencies (LEAs) have sufficient levels of competency to investigate and disrupt the illicit use of VCs. LEAs should develop strategic training programmes for all staff, and should develop a practical baseline technical understanding across front-line officers to support ongoing operations. This can include, for example, training in how to identify cryptocurrency hardware wallets and other related technology that might otherwise go overlooked during an investigation. Expertise-building should include training a greater number of staff in the advanced use of track and trace tools, such as those that are commercially available. Efforts at education and capacity should include training on how to utilise local authorities in the confiscation of virtual currencies, as well as technical training to assist in challenges that arise in undertaking confiscations, such as how to appropriately store seized virtual currencies.

- **Developing an enhanced intelligence picture**. Virtual currencies are feature in a growing range of criminal activity, and the risk landscape is evolving at tremendous speed. Whilst terrorist use of virtual currencies is small compared to that of other illicit actors, the nature of terrorism financing risks that virtual currencies pose could evolve significantly. Member States should conduct risk assessments of virtual currency activity locally, using findings from those assessments to develop strategies for regulatory and law enforcement approaches over the short, medium and long-term. Member States should also develop dedicated virtual currency intelligence taskforces that enable them to obtain multi-disciplinary and holistic

[36] Financial Action Task Force (FATF), ***Financing of the Terrorist Organisation Islamic State in Iraq and the Levant***, February 2015

[37] Financial Action Task Force (FATF), ***Financing of the Terrorist Organisation Islamic State in Iraq and the Levant***, February 2015

[38] Tom Keatinge et al. ***Virtual currencies and terrorist financing: assessing the risks and evaluating responses***, European Union, 2018

intelligence view of the use of virtual currencies across a range of applications and threats. Europol and Member States should ensure that both at an EU-wide level, and locally, efforts to detect and disrupt terrorist use of virtual currencies are closely coordinated with similar efforts related to the detection of cybercrime and the use of virtual currencies by organised crime groups.

- **Enabling public-private partnership.** The public sector cannot develop effective regulation, enhance knowledge and improve intelligence acting alone. Cooperation and interaction with businesses in the virtual currency-industry is essential. Member States should develop dedicated fora for sharing information with local virtual currency industry participants, including sharing of intelligence for operational purposes. At the EU level, Europol should build on its existing efforts and establish dedicated fora for exchanges of operational information between public and private sector stakeholders EU-wide.[39]

In 2019, FATF released a guiding document for a risk-based approach to virtual assets that aims to help countries and virtual asset service providers understand their anti-money laundering and counter-terrorist financing obligations, and effectively implement the FATF's requirements as they apply to this sector.[40]

[39] Tom Keatinge et al. ***Virtual currencies and terrorist financing: assessing the risks and evaluating responses***, European Union, 2018

[40] Financial Action Task Force (FATF), ***Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers***, June 2019

Box 4: Applying new technologies for AML/CTF

New technologies seek to improve the speed, quality, or efficiency and cost of some AML/CTF measures, as well as the costs of implementing the AML/CTF framework more broadly, compared to the use of traditional methods and processes. The technologies of greatest relevance are cross-cutting and enable new digital ways to collect, process, analyse data. These technologies also allow to communicate data and information via a variety of specific solutions. These capabilities can be applied in overlapping ways and target a broad range of AML/CTF objectives. Many of these new technologies' capabilities and implications are still largely unknown. That said, it is essential to understand their current capabilities and potential impact on AML/CTF.

For example, digital identity solutions can enable non-face-to-face customer identification/verification and updating of information. They can also improve authentication of customers for more secure account access, and strengthen identification and authentication when onboarding and transactions are conducted in-person, promoting financial inclusion and combating money laundering, fraud, terrorist financing and other illicit financing activities.

As another example, natural language processing can support more accurate, flexible and timely analysis of customer information and reduce inaccurate or false information and enabling more efficient matching and search for additional data. Better and more up-to-date customer profiles mean more accurate risk assessments, better decision-making, and fewer instances of unintended financial exclusion.

Likewise, Artificial intelligence (AI) and machine learning (ML) technology-based solutions applied to big data can strengthen ongoing monitoring and reporting of suspicious transactions. These solutions can automatically monitor, process and analyse suspicious transactions and other illicit activity, distinguishing it from normal activity in real time, whilst reducing the need for initial, front-line human review. AI and machine learning tools or solutions can also generate more accurate and complete assessments of ongoing customer due diligence and customer risk, which can be updated to account for new and emerging threats in real time.

The adoption of innovative solutions, such as Application Programming Interface (APIs) and Distributed Ledger Technology (DLT), data standardisation, and machine readable regulations can help regulated entities report more efficiently to supervisors and other competent authorities. The technologies also allow alerts, report follow-ups, and other communications from supervisors, law enforcement, or other authorities to regulated entities and their customers, as well as communications among regulated entities, and between them and their customers. The application of more advanced analytics by regulators can also strengthen examination and supervision, including by potentially providing more accurate and immediate feedback.

Source: Financial Action Task Force (FATF), ***Opportunities and Challenges of New Technologies for AML/CTF***, July 2021.

Intercepting terrorist perpetrators and suspects

Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime provides for the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights.[41] Under this Directive, Member States can process, collect, use, and retain PNR data and exchange such data between one another. PNR data contains a large and diverse quantity of data covering the data collected and extracted from various travel documents (usually air flights), and, in general, it can include data contained in passports, telephone numbers, travel carriers, credit card numbers, seat numbers and other elements.[42] In its review report on the PNR Directive, the European Commission draws attention to the fact that it covers the processing of PNR data of all passengers on inbound and outbound extra-EU flights and that such a broad coverage is strictly necessary to achieve the Directive's intended objectives (see Box 5 on the PNR Directive and data protection).[43] The report notes that "the different means of processing of PNR data available (i.e. real time, reactive and proactive) have already delivered tangible results in the fight against terrorism and crime. Qualitative evidence illustrates how the comparison of PNR data against databases and pre-determined criteria has contributed to the identification of potential terrorists […]. In some instances, the use of PNR data has resulted in the arrest of persons previously unknown to the police services, or allowed for the further examination by the competent authorities of passengers who would not have been checked otherwise."[44]

[41] **Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime**

[42] Michele Nino, '**The Protection of Personal Data in the Fight against Terrorism: New Perspectives of PNR European Union instruments in the light of the Treaty of Lisbon**', *Utrecht Law Review*, vol. 6:1 (2010), pp.62–85

[43] European Commission, ***Report from the Commission to the European Parliament and the Council: On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime***, COM(2020) 305, 24 July 2020

Box 5: PNR Directive and data collection

The purpose limitation in the PNR Directive ensures that data processing is only carried out for the objectives of fighting terrorism and serious crime. The prohibition of the collection and processing of sensitive data constitutes an important safeguard to make sure that PNR will not be used in a discriminatory manner. While PNR data may reveal specific information on a person's private life, such information is limited to a specific aspect of private life, namely, air travel. Strict safeguards limit the degree of interference to the absolute minimum and ensure the proportionality of the methods of processing available to national authorities, including as regards the performance of automated processing. As a result of these safeguards, only the personal data of a very limited number of passengers are transferred to competent authorities for further processing. Record-keeping of processing operations enhances transparency and allows to control the lawfulness of data processing in an effective manner. Data Protection Officers can independently control the lawfulness of data processing, in particular when they are not members of the staff of the Passenger Information Unit and are not subordinated to the Head of the Passenger Information Unit. In addition, their presence in the Passenger Information Unit ensures that a data protection perspective is embedded in the daily functioning of these units. On a practical level, the interaction between the Passenger Information Units and their Data Protection Officers appears to be working well and the role of the Data Protection Officer is seen as adding value to the operations of the Passenger Information Unit. The Data Protection Officers play a particularly important role in monitoring data processing operations, approving and reviewing pre-determined criteria and providing advice on data protection matters to the staff of the Passenger Information Unit. In most Member States, the Data Protection Officers have been designated by law as the contact point for data subjects and contacting them is also facilitated in practice.

Source: European Commission, ***Report from the Commission to the European Parliament and the Council: On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime***, COM(2020) 305, 24 July 2020.

UN Security Council Resolution 2322 adopted in December 2016 called upon states to share, where appropriate, information about foreign terrorist fighters and other individual terrorists and terrorist organisations,

[44] European Commission, ***Report from the Commission to the European Parliament and the Council: On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime***, COM(2020) 305, 24 July 2020

including biometric and biographic information, as well as information that demonstrates the nature of an individual's association with terrorism via bilateral, regional and global law enforcement channels, in compliance with international and domestic national law and policy.[45] This Resolution also stressed the importance of providing such information to national watch lists and multilateral screening databases. UN Security Council Resolution 2396 (2017) adopted under Chapter VII of the UN Charter, decided that Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law.[46] This Resolution underlined the importance of international, regional, and state-to-state cooperation in setting up systems for biometric data collection and encouraged states to share such data responsibly among one another, as appropriate, and with INTERPOL and other relevant international bodies. Since the adoption of these two resolutions, the use of biometrics for counter-terrorism purposes – notably in the context of border management and security – has become increasingly widespread: "Biometrics have become more prevalent in efforts to detect criminals, known terrorists, and individuals suspected of terrorist offences, including in public spaces, with facial recognition systems used in conjunction with CCTV video surveillance. Recognition technology has also been coupled with unmanned aircraft systems (UAS) in a law enforcement and border control context, helping to control large crowds and assist in the identification of individuals in public spaces."[47]

[45] United Nations Security Council, **Resolution 2322 (2016)**, S/RES/2322 (2016), 12 December 2016

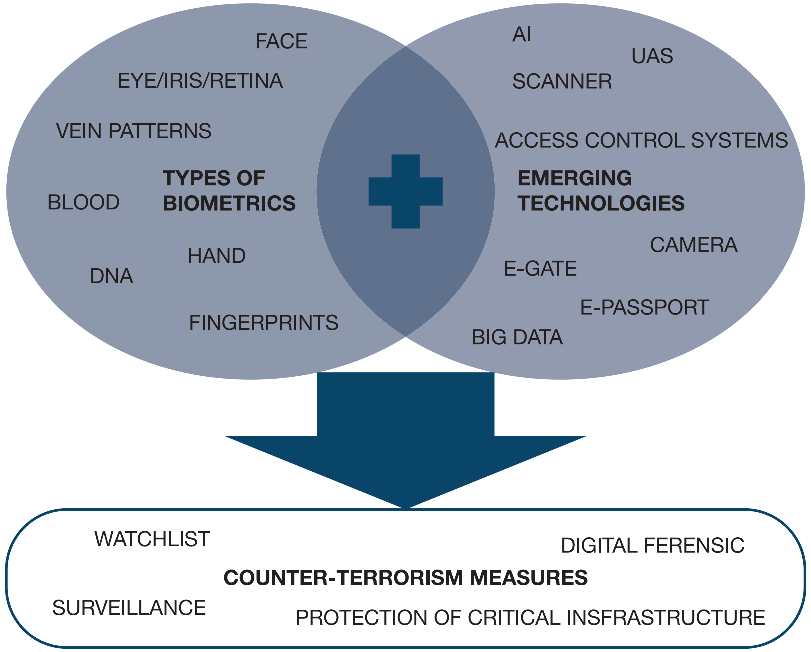
[46] United Nations Security Council, **Resolution 2396 (2017)**, S/RES/2396 (2017), 21 December 2017

[47] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), ***CTED Analytical Brief: Biometrics and Counter-Terrorism***, December 2021

A recent analysis by the UN Security Council Counter-Terrorism Committee Executive Directorate (CTED) notes that: "The use of biometrics in counter-terrorism is often connected to the development and utilization of emerging technologies. This has included techniques to identify individuals of interest – for example high-definition cameras, matching algorithms, and artificial intelligence (AI), sometimes in conjunction with a linked database (e.g., terrorist watchlists) – and the use of biometrics (including multi-biometrics access control systems) to protect critical infrastructure sites and facilities, as well as 'soft' targets, from terrorist attacks" (Figure 2).[48]

[48] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), ***CTED Analytical Brief: Biometrics and Counter-Terrorism***, December 2021

Figure 2: Trends in biometric data collection for counter-terrorism



Source: UNSC CTED, *CTED Analytical Briesf: Biometrics and Counter-Terrorism*, December 2021.

To facilitate the responsible use and sharing, in 2018 CTED and the UN Office of Counter-Terrorism compiled a compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism.[49] This document provides information regarding the governance and regulatory requirements for biometric technology from the perspective of international law, human rights law, ethical reviews, data protection, and the right to privacy. It also discusses the potential vulnerabilities of biometric systems and some of the control measures that can be used to mitigate related risks. International technical and scientific operating standards are also considered. The compendium provides a general overview of current counter-terrorism biometric systems and databases across the spectrum of law enforcement, border management, and military applications.[50] The European Union Agency for Fundamental Rights (FRA) has examined the fundamental rights implications of using facial recognition technology for law enforcement purposes highlighting a set of considerations to be addressed before such systems are deployed (Box 6).[51] Civil society groups have also voiced concerns regarding fundamental rights over biometric surveillance.[52] In a joint 2020 statement regarding the EU Counter-Terrorism Agenda, several non-governmental organisations cautioned against the unfettered use of facial recognition technology and called for an inclusive multi-stakeholder dialogue to help ensure robust fundamental rights protection.[53] A 2021 analysis by CTED points out that stakeholders face persisting challenges regarding the responsible use of biometric data, including:

- Technological weakness and limitations.
- Insufficient capacity.

[49] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter-Terrorism, ***United Nations Compendium of Recommended Practices for Responsible Use and Sharing of Biometrics in Counter-Terrorism***, 2018

[50] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter-Terrorism, ***United Nations Compendium of Recommended Practices for Responsible Use and Sharing of Biometrics in Counter-Terrorism***, 2018

[51] European Union Agency for Fundamental Rights, ***Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement***, 27 November 2019

[52] European Center for Not-for-Profit Law, ***Upholding Human Rights in Regulation and Use of Biometric Technology in Counter-Terrorism Law and Practice***, 25 June 2021. See also Privacy International, ***Biometrics Collection under the Pretext of Counter-Terrorism***, 28 May 2021

[53] Article 19, European Digital Rights (EDRi), and Hermes Center, ***Statement: Civil Society Challenges EU Plans to Expand Biometric Mass Surveillance***, 14 December 2020. See also Privacy International, ***The EU Parliament Took a Stance Against AI Mass Surveillance: What are the Global Implications?***, 20 October 2021

- Insufficient legal and administrative frameworks.
- Insufficient oversight, safeguards, and protection of privacy and data, and the duration of data retention.
- Reinforcement of existing discrimination and inequalities.
- Potential misuse and challenges to protected freedoms of religion, expression, and association.
- Limited sharing of biometric data and information.
- Lack of effective remedies in case of violations.
- Risk of fraud and abuse of biometric data.[54]

[54] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), ***CTED Analytical Brief: Biometrics and Counter-Terrorism***, December 2021

Box 6: Facial recognition technology in law enforcement: a fundamental rights perspective

The fundamental rights implications of using facial recognition technology vary considerably depending on the purpose, context and scope of the use. Some of the fundamental rights implications stem from the technology's lack of accuracy. Accuracy has strongly increased, but the technology still always comes with a certain rate of error, which can negatively impact fundamental rights. Moreover, importantly, several fundamental rights concerns would remain even if there were a complete absence of errors.

Fundamental rights considerations notwithstanding the context, purpose, and scope of use of facial recognition technology

- The rights to respect for private life and protection of personal data are of utmost importance. The way facial images are obtained and used – potentially without consent or opportunities to opt out – can have a negative impact on people's dignity.
- Any use of the technology needs to be thoroughly assessed in terms of its potential impact on non-discrimination and rights of special groups, such as children, older persons and persons with disabilities, because of the (sometimes unknown) varying accuracy of the technology for these groups and according to other protected characteristics.
- Freedom of expression, association and assembly must not be undermined by the use of the technology.
- It is essential to consider procedural rights when facial recognition technology is used by public administrations, including the right to good administration and the right to an effective remedy and fair trial.

Source: European Union Agency for Fundamental Rights, ***Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement***, 27 November 2019.

Communications surveillance is another common element of counter-terrorism strategies. FRA distinguishes between three approaches for communications surveillance.[55] General surveillance of communications means that intelligence can be collected with technical means and at a wide scale. This surveillance technique is referred to in different ways, including 'signals intelligence', 'strategic surveillance', 'bulk investigatory powers', 'mass digital surveillance' and 'storage of data on a generalised

[55] EU Agency for Fundamental Rights, ***Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the European Union – Volume II***, 2018

basis'. Targeted surveillance presupposes the existence of prior suspicion of a targeted individual or organisation. Untargeted surveillance starts without prior suspicion or a specific target. Oversight is crucial to ensure that intelligence services are held accountable for their actions and encourage the development of effective internal safeguards within the services.[56]

The 'International Principles on the Application of Human Rights to Communications Surveillance' published in 2013 by a group of civil society groups, industry and international experts focus on how existing human rights law applies to communications surveillance technologies and techniques (Box 7).[57] For the purposes of these principles, communications surveillance encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future.[58] The principles apply regardless of the purpose for the surveillance – law enforcement, national security or any other regulatory purpose.

[56] EU Agency for Fundamental Rights, ***Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the European Union – Volume II***, 2018

[57] Anja Kovacs and Dixie Hawtin, ***Cyber Security, Cyber Surveillance and Online Human Rights***, Global Partners Digital, 31 January 2013

[58] Necessary and Proportionate, ***International Principles on the Application of Human Rights to Communications Surveillance***, 10 July 2013

Box 7: International Principles on the Application of Human Rights to Communications Surveillance

Legality

Any limitation to the right to privacy must be prescribed by law. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

Legitimate aim

Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Necessity

Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights.

Adequacy

Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

Proportionality

Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

Competent judicial authority

Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.

Due process

Due process requires that individuals' human rights are respected and guaranteed by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.

User notification

Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation.

Transparency

States should be transparent about the use and scope of communications surveillance techniques and powers. They should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance.

Public oversight

States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

Integrity of communications and systems

In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes.

Safeguards for international cooperation

The mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied.

Safeguards against illegitimate access

States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals.

Source: Necessary and Proportionate, ***International Principles on the Application of Human Rights to Communications Surveillance***, 10 July 2013.

The potential of data mining and automated data analysis tools for counterterrorism has long been examined. Data mining refers to the process that uses algorithms to discover predictive patterns in data sets and automated data analysis applies models to data to predict behaviour, assess risk, determine associations, or do other types of analysis.[59] These models can be based on patterns (from data mining or discovered by other methods) or subject based, which start with a specific known subject. Whereas the use of such tools is viewed as a way to facilitate terrorist profiling, it is essential to consider whether protections for privacy are adequate to address the negative consequences of increased government use of private data. Decisions concerning the application of such tools should be made in an open and transparent manner. At the same time, some commentators have suggested that technology itself may provide solutions for addressing challenges related to privacy and liberties.[60] One example is privacy-preserving datamining (PPDM) which "refers to datamining computations performed on the combined data sets of multiple parties without revealing each party's data to the other parties. The data consist of possibly overlapping sets of variables contained in the separate data bases of the parties and overlapping sets of individuals."[61] PPDM does not come without criticism though: "A major problem with the PPDM literature is that the so-called proofs of security are designed not to protect the individuals in the database but rather the database owners, as in the case of two companies sharing information but not wanting to reveal information about their customers to one another beyond that contained in the shared computation. Once the results of the datamining consist of linked extracts of the data themselves, however, the real question is whether one of the parties can use the extra information to infer something about the individuals

[59] Mary DeRosa, ***Data Mining and Data Analysis for Counterterrorism***, CSIS, 2004

[60] Mary DeRosa, ***Data Mining and Data Analysis for Counterterrorism***, CSIS, 2004

[61] Stephen E. Fienberg, ***Homeland Insecurity: Datamining, Terrorism Detection, and Confidentiality***, Technical Report No 148, National Institute of Statistical Sciences, December 2004

in the other party's data that would otherwise not be available."[62] The application of AI for predictive counterterrorism raises similar issues (Box 8). Civil society groups in Europe have systematically oppose to the use of AI and automated decision-making (ADM) for the purposes of predicting criminal activities, including criminal profiling and risk assessment noting that such technologies can reinforce and reproduce biases and discrimination.[63] As a result, vulnerable social groups can be disproportionately targeted by law enforcement services.

Box 8: AI prediction in counterterrorism: cost-benefit considerations

The way in which AI capabilities are used for predictive purposes in countering terrorism is critical. The current constructs that regulate the use of predictive AI in countering terrorism seem unlikely to either safeguard against misuse or to enable the most beneficial use of these technologies, both in terms of operational performance and adherence to human rights principles.

Pursuing more concerted efforts to use predictive AI in counterterrorism operations would require commitment in terms of research and experimentation, in order to develop models that are ready to use. If AI technologies for predicting terrorism reach maturity, greater data access and centralisation – under strict safeguards – could offer a way of mediating infringement of privacy to proportionate ends.

The fact that AI makes invasion of privacy at scale much easier means that the use of those technologies remains a public policy concern. How successfully states manage the powers that new technology brings them will continue to reflect how well established their institutions are, and the strength of their commitment to protecting citizens' rights in general.

Source: Kathleen McKendrick, ***Artificial Intelligence Prediction and Counterterrorism***, Chatham House, August 2019.

[62] Stephen E. Fienberg, ***Homeland Insecurity: Datamining, Terrorism Detection, and Confidentiality***, Technical Report No 148, National Institute of Statistical Sciences, December 2004

[63] Fair Trials, ***Automating Injustice: Artificial Intelligence and Automated Decision-Making in Criminal Justice***, 9 September 2021. See also Fair Trials and European Digital Rights (EDRi), ***Civil Society Calls on the EU to Ban Predictive AI Systems in Policing and Criminal Justice in the AI Act***, 1 March 2022

Community-based Approaches for Preventing Violent Radicalisation

In 2003, the Congress of Local and Regional Authorities in Europe (CLRAE), an institution of the Council of Europe, responsible for strengthening local and regional democracy and assessing the application of the European Charter of Local Self-Government adopted a Resolution on the role and responsibilities of local authorities in tackling terrorism.[64] This Resolution noted that the fight against terrorism is "a political and public priority requiring constant and extensive vigilance, co-ordination between a range of partners, effective legislation against violence and a determined and proactive judicial and political approach to racial and religious intolerance and extremism." It stressed that "the protection of human rights and civil liberties should be seen as an integral part of the struggle against terrorism, not as an obstacle to it; that the fundamental values of human rights and dignity must not be sacrificed in the combat against terrorism; and that anti-terrorism measures should be reasonable, proportionate and non-discriminatory." The Resolution further affirmed that it is essential "to avoid discriminatory legislation; arbitrary prolonged detention sometimes without trial; the definition of certain peaceful activities as terrorism; unnecessary increased surveillance powers; and erosion of rights at trials." To fulfil these goals, the Resolution identified several lines of actions and called upon local authorities to take appropriate steps for their implementation (Box 9). It is evident from the proposed lines of action that the CLRAE recognises the importance of a holistic approach to countering violent extremism that is grounded in community engagement and empowerment, dialogue, and ongoing crisis prevention and management.

[64] Congress of Local and Regional Authorities, **Resolution 159 (2003) on tackling terrorism – the role and responsibilities of local authorities**, 22 May 2003

Box 9: Tackling terrorism – the role and responsibilities of local authorities

The Congress of Local and Regional Authorities asks local authorities in Europe to:

– A. Devise strong and clear policies to:

- foster social cohesion and eradicate social exclusion;
- promote tolerance through educational and cultural programmes;
- ensure respect for cultural diversity and the peaceful coexistence of different cultures, minorities and communities;
- prevent residential or educational segregation.

– B. Seek to address in an equitable manner social, political and economic problems in their populations and ensure fair and equal access to public utilities and educational and employment opportunities;

– C. Encourage and promote regular dialogue between different religious faiths, in other words between their leaders, institutions and communities, ensuring that equal conditions exist for the practice of each faith.

– D. Remain vigilant and, in particular, take all necessary steps, to protect people in places where they gather and in partnership with specialised agencies and governments, to protect major civil and industrial and nuclear installations.

– E. Fully inform the public about all threats and risks, planned contingency measures and subsequent crisis management.

– F. Take all necessary steps to ensure the co-ordination of emergency services, ensuring that:

- the chain of command, accountability and responsibilities are clearly defined;
- there is a back-up supply of basic services, communications and infrastructure which can be used in the event of a crisis;
- adequate training exercises and response simulations are organised in advance.

Source: Congress of Local and Regional Authorities, **Resolution 159 (2003) on tackling terrorism – the role and responsibilities of local authorities**, 22 May 2003.

The complementary role of community engagement and community-oriented policing as tools for building trust with local communities and engaging with them as partners to develop information-driven community-based solutions to the threat of violent extremism has also been acknowledged by the Global Counter-Terrorism Forum (GCTF).[65]

The TERRA Toolkit is an example of a flagship initiative that aims to facilitate multi-stakeholder engagement for tackling violent radicalisation.[66] This Toolkit is primarily intended to support existing or new networks of teachers, youth workers, law enforcement officers, religious leaders and local policy-makers as they exchange information on young people at risk of radicalising, and to come to a weighted judgment on the risks. It also informs journalists and policy-makers on influences they may have on the background factors that lead to radicalisation. The toolkit comprises (1) a general background document which covers the objectives, presuppositions and starting points, implications for use and implementation; (2) separate tools for each target group with manuals on the indicators of radicalisation and tip sheets; and (3) video material showing testimonials from victims of terrorism, former radicals and interviews with representatives of the different target groups.[67]

The Aarhus Model applied in Denmark comprises programmes in support of both the early prevention of violent radicalisation and exit processes.[68] Prevention strategies are aimed at youngsters who do not yet

[65] Global Counter-Terrorism Forum, ***Good Practices on Community Engagement and Community-Oriented Policing as Tools to Counter Violent Extremism***

[66] RAN Collection**, TERRA Toolkit**

[67] **TERRA Toolkit** – Community Approach to Radicalisation

[68] Preben Bertelsen, **'Danish Preventive Measures and De-Radicalisation Strategies: The Aarhus Model'** in Wilhelm Hofmeister and Megha Sarmah (eds.), *From the Desert to World Cities: The New Terrorism*, Konrad-Adenauer-Stiftung, 2015

represent any danger or security risk but may become dangerous if their radicalisation process continues in a violent direction. Exit strategies are aimed at radicalised individuals with intentions and capabilities to engage in violent crime and terrorism. The Aarhus does not address a specific ideology; rather, it uses the principle of inclusion as a basis for transforming the personal, social, cultural and political motivations of disgruntled or radicalised individuals into legal modes of participation and citizenship.[69] Whilst the overall effectiveness of the Aarhus Model depends largely on the level of motivation of participating individuals to undergo a cognitive transformation and avoid violent behaviour, the functioning of this model requires community vigilance and support, including ability among first-line practitioners in different sectors to recognise and report radicalisation risks.

[69] Preben Bertelsen, **'Danish Preventive Measures and De-Radicalisation Strategies: The Aarhus Model'** in Wilhelm Hofmeister and Megha Sarmah (eds.), *From the Desert to World Cities: The New Terrorism*, Konrad-Adenauer-Stiftung, 2015

Conclusion

This report has focused on the use of hybrid investigations and data collection in the context of counter-terrorism. In doing so, the report has reviewed the concept of preventive policing, existing models for identifying extremist behaviour on the internet, and the application of novel technologies for countering terrorism financing and intercepting and apprehending terrorist suspects and perpetrators. Key cross-cutting themes include the need for broad-stakeholder engagement and ensuring effective fundamental guarantees in the development and implementation of counter-terrorism policies, strategies, and tools. Community-based approaches for preventing radicalisation that bring together and empower front-line practitioners with skill to recognise and flag radicalisation risks can play a vital role in facilitating early intervention processes and thus contribute to strengthening counter-terrorism.

PRE-RIGHTS

This project is co-funded
by the European Union's
Justice Programme (2014-2020)