Norwegian Ministry
of Foreign Affairs

GCSD

PREVENTING AND COUNTERING VIOLENT EXTREMISM:

A handbook of international best practices

Norwegian Ministry
of Foreign Affairs

GCSD

PREVENTING AND COUNTERING VIOLENT EXTREMISM:

A handbook of international best practices

Eden Cole

Georgian Center for Strategy and Development (GCSD) is a non-profit, non-partisan, non-governmental organization, which intends to support Georgia's national security, to strengthen principles of effective and democratic governance of the country and to create conditions for Georgia's sustainable development. Based on the goals of the center, its work involves research, monitoring, advocacy and implementation of educational projects.

With the support of the Ministry of Foreign Affairs of the Kingdom of Norway, GCSD is currently implementing a four-year multi-tier program on 'Enhancing the Capacity of Georgia in Preventing Violent Extremism and Radicalization'. To date, this preventing and countering violent extremism (P/CVE) program has produced a series of useful knowledge products and guidance material on P/CVE issues, including manuals for both Media and Civic Education Teachers, and an introductory guide to P/CVE Concepts, Programming, and Best Practices. GCSD has also managed and implemented P/CVE capacity development programming, including capacity building for CSOs, civil servants, and media.

This Handbook was developed to benefit Georgia's Permanent Interagency Commission on Elaboration of the National Counterterrorism Strategy (CNCS) to facilitate P/CVE policy development and cooperative programming.

In a field crowded with documentation and narratives on diverse P/CVE approaches, the intention of this Handbook is to focus the audience's attention on counter-terrorism and P/CVE best practice, not only at international, but also at European levels. At the same time, the Handbook enables practitioners from state institutions to sustain institutional P/CVE knowledge and to develop capacity to address P/CVE issues across Georgian society. The Handbook can also be used for training purposes, as well as by other stakeholders to develop their own capacity to implement projects aimed at understanding and limiting the threat of violent extremism.

Beginning with an introduction to the evolution of terrorism over the last fifty years, the Handbook proceeds to outline the challenges of terrorism to democratic states, and the legal and policy dimensions of effective counter-terrorism and extremism prevention. The Handbook then moves to address specific thematic issues, including institutional frameworks for P/CVE, cooperation between state and society, radicalization prevention, the return of foreign terrorist fighters and their families, and broader counter-terrorism and P/CVE communication challenges. Placing an emphasis on developing original material and incorporating a variety of relevant and easily accessible best practice materials, the aim across all seven chapters is to ensure that a 'Whole-of-Society' approach to P/CVE issues is emphasized in a user-friendly format.

Against the background of fifty years of terrorism, democratic societies are still exposed to a variety of risks posed by local and strategic terrorism. Although waves of terrorism tend to occur in peaks and troughs, as contested and ungoverned spaces continue to harbor often well-funded and supplied terrorist and insurgent groups, social and technological developments compound the significant risks posed by even small terrorist movements and cells. To counter these threats, the legal and policy framework for counter-terrorism and counter-extremism programming will continue to evolve, not least to disrupt online terrorist recruitment, communication, and radicalization activities, and also to limit the transit of terrorists across international travel networks. In this context, every democratic society faces the dual challenge of maintaining their preparedness to counter terrorist threats, and to adapt their P/CVE approaches to contain new or persistent terrorist threats.

In the interim, Georgia, as with other European democracies, will remain exposed to a variety of counter-terrorism and P/CVE challenges. Limiting Georgia's exposure to international terrorist networks, creating effective counter-terrorism policy, ensuring effective P/CVE practice, and enhancing Georgia's cooperative security efforts will require further development of existing P/CVE capacities, particularly in terms of maintaining substantive institutional and multi-stakeholder approaches to terrorist and radicalization threats. In so doing, Georgia will continue to contribute to European and international security.

TABLE CONTENTS

Chapter One: Political Violence, Terrorism, Violent Extremism, Radicalisation 4
Chapter Two: Challenges of counterterrorism in a democratic state 15
Chapter Three: Institutional Frameworks 28
Chapter Four: Radicalisation Prevention 38
Chapter Five: Cooperation between State and Society in P/CVE 48
Chapter Six: Returnees 56
Chapter Seven: Communication 65

Norwegian Ministry
of Foreign Affairs

GCSD

Chapter One: Political Violence, Terrorism, Violent Extremism, Radicalisation

Introduction

> *Acts of terrorism constitute one of the most serious violations of the universal values of human dignity, freedom, equality and solidarity, and enjoyment of human rights and fundamental freedoms on which the Union is founded. They also represent one of the most serious attacks on democracy and the rule of law, principles which are common to the Member States and on which the Union is based.*[1]
>
> Article 2, EU Directive 2017/541 of the European Parliament and of the European Council of 15th March 2017 on Combating Terrorism

Terrorism as we know it today emerges in the second half of the nineteenth century. After a bomb exploded outside Clerkenwell's New Prison in London in 1867, a later Irish Republican bombing campaign from 1881 to 1885 featured dynamite attacks on military and police barracks, Scotland Yard, trains and stations on the original London Underground, the offices of The Times newspaper, and the headquarters of the Special Branch. Further east, following the bombing of the Winter Palace in 1880 and a failed dynamite plot on the Imperial Train, in 1881 Tsar Alexander II of Russia was assassinated by bomb-throwing Russian nihilists of 'Narodnaya Volya' as he returned to the Winter Palace in a carriage.

By the close of the century, the nihilist Peter Kropotkin reflected in *Memoirs of a Revolutionist* that:

> Terrorism was called into existence by certain special conditions of the political struggle at a given historical moment. It has lived, and has died. It may revive and die out again[2].

Kropotkin's observation remains apt to this day. Within twenty-five years of Kropotkin writing, the outcome of respective state responses to these and much broader political challenges in Imperial Russia and the United Kingdom would lead– via the 1905 Winter Palace and 1916 Easter Rising – to the 1917 Bolshevik Revolution and the establishment of the Irish Free State.

In this chapter the origins and key features of contemporary terrorism are outlined and defined. The chapter surveys the evolution of terrorism from the 1970s through to the 2000s, and then maps contemporary terrorist challenges. The chapter then outlines the key challenges of strategic terrorism and defines key elements of what can be assessed as terrorism or terrorist activities.

Overall, the features of terrorism in the late nineteenth century – attacks on high profile political, economic, business, or infrastructure targets, disruption of communications, civilian casualties, and assassinations remained a constant for over a century. At the same time, Kropotkin's observation remains valid in so far as some terrorist networks can thrive, but can then disappear as quickly as they emerged, a disappearance often conditioned by the nature of the state response to terrorism itself.

[1] Directive (EU) 2017/541 of the European Parliament and of the Council of 15th March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, available at: http://data.europa.eu/eli/dir/2017/541/oj and https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32017L0541

[2] Peter Kropotkin, *Memoirs of a Revolutionist*, Chapter 12, (Cosimo, 2009), p. 297, available at: https://books.google.ch/books?id=9nvlvlXnMSkC&printsec=frontcover&hl=de&source=gbs_ge_summary_r&cad=0#v=onepage&q=terrorism&f=false

Defining Terrorism

'Terrorism' is used to refer to specific violent acts that cannot be categorised as sustained acts of conventional or limited warfare or low intensity conflict, such as guerrilla warfare used by popular resistance movements, to fight against a state's forces. In the mid-1980s, terrorism could be simply defined by Professor Paul Wilkinson as:

> the systematic use of murder, injury and destruction or threat of same to create a climate of terror, to publicise a cause and to intimidate a wider target into conceding to the terrorists' aims[3]

In the 2000s, Professors Peter Neumann and Michael Smith have refined the definition further to preliminarily describe terrorism as:

> the deliberate creation of a sense of fear, usually by the use or threat of use of symbolic acts of physical violence, to influence the political behaviour of a given target group[4]

This definition is based on terrorism's three distinguishing features: the violent nature of most acts of terrorism; the nature of the violence employed in an act of terrorism; and the symbolic character of the act of violence.

Firstly, the violent quality of most terrorist acts distinguishes a programme of terror from other forms of non-violent propagation or direct action, such as mass demonstrations and protests, leafleting, and strikes by workers in different professions. Although people will sometimes experience fear and anxiety without a threat of physical harm being present, it is apparent that the most common vehicle for the inducement of terror is forms of physical violence or simply the threat of exposure to random violence.

Secondly, the nature of the violence itself distinguishes terrorism from other forms of conflict. Neumann and Smith draw on Thornton's phrase describing the violence as 'extra-normal', meaning that for a certain level of organized political violence to be called terrorism, the violence must go beyond the norms of violent political agitation accepted by a particular society. The level of violence is atypical or abnormal for a civilised society, as are the means.

Thirdly, the act of violence has a symbolic character. An act of terror will imply a broader meaning than the immediate effects of the act itself: the damage, disruption, deaths, and/or injuries caused by the act of violence are of limited relevance to the political message which a terrorist hopes to communicate via national and international media, social media, and its own internal communication channels. For this reason, the terrorist act can be understood by appreciating its symbolic content or 'message'[5]. This is particularly apt today when thinking of the fundamental role of the 'violent image' in terrorist propaganda across social media channels.

This final point emphasises a key element of terrorism, that it is by its very essence a particular form of psychological warfare, 'a battle of wills played out in people's minds'[6]. By creating a sensation of fear in a population or target group, terrorism – like other forms of organized political violence – is employed to produce certain effects on a specific set of people in order to attain an objective of policy: terrorism is a

[3] Paul Wilkinson, 'Terrorism and the Rule of Law', *Harvard International Review*, May/June 1985, p. 12, cited in: Paul Wilkinson, 'International Terrorism: the Changing Threat and the EU's response', EU-ISS, *Chaillot Paper*, No. 84, October 2005, available at: https://www.iss.europa.eu/content/international-terrorism-changing-threat-and-eu%E2%80%99s-response

[4] Peter Neumann and M. L. R. Smith, 'Strategic Terrorism: The Framework and its Fallacies', *Journal of Strategic Studies*, Vol. 28., No. 4., August 2005, p. 574.

[5] T. P. Thornton, 'Terror as a Weapon of Political Agitation', in Harry Eckstein (ed.), *Internal War: Problems and Approaches*, (New York: Free Press 1964), pp. 71–99, cited in: Neumann and Smith, 'Strategic Terrorism', p. 575.

[6] Gerard Chaliand, *Terrorism: From Popular Struggle to Media Spectacle*, (London: Saqi Books, 1987), pp.107–12, cited in Neumann and Smith, 'Strategic Terrorism', p. 576.

violent attempt at coercion[7].

Subjectively, there is ambiguity about how to define a level of fear. In extremes, people can adapt to a perceived threat, but the everyday disruption caused by additional security measures imposes increasing costs on society, government, and changes behaviours, particularly in a previously stable, peaceful, and law-abiding society. The level of terror or fear may lessen or dissipate after a terrorist campaign ends or if it continues for a long time. But, if this occurs, terrorists can simply sustain an atmosphere of defiance rather than fear and anxiety[8]. The strategic capacity of terrorists to adapt to changing political and social environments, and for societies to counter them, is addressed in the following sections and chapters.

Collectively, these points emphasise terrorism's impact on society as a whole; to adopt necessary preventative measures there is a need not only for whole-of-government approach but also for a whole-of-society approach to limit society's vulnerability to acts of terrorism. The enduring challenge of terrorism is that the nature of the state response to terrorist incidents can determine longer term political outcomes and bring into sharp focus the legitimacy of state institutions.

European Definitions

The precise definitions of terrorism outlined in the previous section are reflected in practical definitions in contemporary legislation and international guidance that feed into national government's policy and practice. In order to orient stakeholders on European Union (EU) current practice, this section briefly overviews the state of play in the EU to outline the consensus on what constitutes terrorist activity, before moving to definitions of other relevant concepts. These definitions will also be addressed in terms of policy and legal challenges in Chapter Two.

European Union member states originally agreed a minimum definition in the 2002 'EU Framework Decision on Combating Terrorism', and the harmonised definition of terrorist offences listed in Article 1 has served as the cornerstone for subsequent decisions and regulations. For the purposes of international co-operation between EU member states, the definition sets out a comprehensive list of intentional criminal acts – ranging from murder, to kidnapping, hijacking, infrastructure attacks, and threats to commit any such acts – that must be considered as terrorist acts if they have any of the following objectives:

- to seriously intimidate a population; or
- to unduly compel a government or international organization to perform or abstain from performing any act; or
- to seriously destabilise or destroy the fundamental structures of a country or an international organisation.[9]

The definition of a "terrorist group" in the following Article reflects the often limited size and limited time duration of particular terrorist groups or cells:

> 'a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences'[10].

[7] Neumann and Smith, 'Strategic Terrorism', p. 576.

[8] Neumann and Smith, 'Strategic Terrorism', p. 575.

[9] EU Council Framework Decision of 13 June 2002 on combating terrorism, (2002/475/JHA), OJ L 164, 22/06/2002, Art. 1(1), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002F0475

[10] EU Council Framework Decision of 13 June 2002 on combating terrorism, Article 1.

The term "Structured group" is also flexibly defined to mean a terrorist group:

> ‘that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure[11]’.

The 2017 Directive addresses the rapid evolution of terrorist threats over the last decade, addressing the travel and return of ‘Foreign Terrorist Fighters’, principally citizens, more comprehensive measures against various types of terrorist financing and illicit trafficking, the role of intermediaries in supplying services to terrorist groups, removing online content soliciting terrorist offences, and against training provision and recruitment for the purposes of terrorism[12]. While the Framework Decision harmonises a minimum threshold for offences to be classified as terrorist offences, it does not prevent EU member states from having a more extensive definition of terrorism in their national laws.

Similarly, although the 2005 Council of Europe Convention on the Prevention of Terrorism did not define terrorism, it required all member states to create new criminal offences in relation to acts that may lead to terrorism offences as per established by the UN treaties and protocols on terrorism. Under the Convention, member states have to extradite and/or prosecute in relation to the new preparatory offences created under the Convention, a key element of effective counter terrorism cooperation.

This established consensus of what constitutes terrorism provides any government with a clear roadmap for taking preventative measures and prosecutions. The consensus also reflects an aggregate of lessons learned over previous generations. While the specific measures governments and wider societies can take to counter terrorism are the subject of the following chapters, the subsequent sections of this chapter outline key concepts, states’ experience of terrorism, and terrorist group’s strategies in order to contextualise the broad framework in which effective counter terrorism can be better understood.

Key Concepts

During the 2000s, the international community moved its focus from solely countering terrorism towards preventing terrorism. Similar and sometimes duplicative terminology has proliferated, but describes the same concepts. The concepts remain important as they cumulatively describe preventative best practice advocated from United Nations to European (including Council of Europe, EU, and OSCE) to national levels. OSCE’s guidance is useful as it reflects a consensus on international and regional best practice, and can be used to outline key concepts in a structured format.

Underlying the more useful strategies for addressing what OSCE cumulatively describes as ‘Violent Extremism and Radicalisation that Lead to Terrorism’ (**VERLT**) is the belief that the ‘radicalisation’ process through which individuals accept the use of violence as legitimate for political purposes is non-linear and multi-causal. Therefore, any approach which seeks to address VERLT should be holistic in nature, an understanding often expressed worldwide as Countering Violent Extremism (**CVE**), and in some instances as Preventing Violent Extremism (**PVE**), that contrasts with traditional hard security-based approaches known as Counter-Terrorism (**CT**) which primarily focus on increasing the technical capacity of security providers. For the purposes of this handbook, the acronym **P/CVE** will be used to refer to both CVE and PVE.

In this vein, OSCE emphasises preventative rather than reactive measures in regard to terrorism. This approach entails a focus on the ‘root causes’ of terrorism, as well as the structural factors that can create

[11] EU Council Framework Decision of 13 June 2002 on combating terrorism, Article 2.

[12] Directive (EU) 2017/541 of the European Parliament and of the Council of 15th March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Articles 8-19, available at: http://data.europa.eu/eli/dir/2017/541/oj and https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A32017L0541

a climate conducive to its promotion and use. In this context, the OSCE focuses both on CVE-relevant initiatives, as well as CVE-specific initiatives—a distinction made to differentiate those activities that aim to address the structural drivers of violent extremism (e.g. CVE-relevant initiatives, such as human rights training for security providers), against those tailored directly against violent extremism or vulnerable individuals (e.g. CVE-specific initiatives, such as conferences exploring best practices in the prevention of terrorist radicalisation in prisons)[13].

Consequently, OSCE – in common with other regional organisations – focuses primarily on addressing the '**push-factors**' that drive an individual to turn to violence, rather than the '**pull-factors**' which attract an individual to violent extremist network[14]. 'Push-factors' are centred around the concept of grievances (both real and imagined), such as social, political, ethnic, or cultural injustice or discrimination, while 'pull-factors' primarily concerns the psychological motivations of groups and individuals, such as the desire to belong to a cause, ideology, or a social network.

The terminology outlined above will be used throughout the handbook, with particular reference to P/CVE.

Terrorism in Contemporary History

For the last forty years many of terrorism's key features have remained constant, even as terrorists have adapted their tactics, strategy, and use of technology. This section overviews some of the key drivers of terrorism and the foundation of contemporary 'strategic terrorism'.

1970s – 1990s

In the aftermath of World War Two, a variety of mass resistance and revolutionary movements accelerated decolonisation processes in Africa and Asia, but Western European nations were not affected by domestic terrorist campaigns. However, by the 1970s, terrorism re-emerged. The origins – or triggers – for terrorist campaigns initially reflected a variety of grievances that then sustained – and in some cases escalated – terrorist violence.

In Northern Ireland, discrimination by a Protestant majority against a Roman Catholic minority in terms of civil rights, including voting rights, access to services, housing, and job opportunities led to the emergence of a popular protest and subsequent resistance movement in the late 1960s. Rioting that occurred after Roman Catholics were attacked and driven from their homes led to the emergence of paramilitary units such as the Provisional IRA (PIRA).

In West Germany, a disaffected young generation of political active students radicalised by revolutionary ideology, the Vietnam War, national politics, and the murder of a protestor by Berlin's police during a visit by the Shah of Iran, led a small number of activists in the Extra-Parliamentary to collaborate in ad hoc groups including the Movement of the 2nd June, Revolutionary Cells, and, most notorious of all, the Red Army Faction (RAF).

Terrorists trained in the Middle East also launched campaigns across Europe, with the Popular Front for the Liberation of Palestine (PFLP) focused on aircraft hijackings, and other groups attacking the 1972 Munich Olympics (Black September), and seizing hostages at a 1975 OPEC meeting in Vienna (Arm of the Arab Revolution). Terrorist networks were also internationalising: the Japanese Red Army and German

[13] Eden Cole and Richard Steyne, Mapping Study on 'Strengthening OSCE's Role in Central Asia: Combatting Violent Extremism by Applying Human Security Measures', (Geneva: August 2017), p. 7. Also see Peter Neumann, 'Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region', OSCE, CIO.GAL/189/17, (September 2017) p. 38, available at: https://www.osce.org/chairmanship/346841

[14] Cole and Steyne, 'Mapping Study', p. 7.

RAF both trained at PFLP training camps. At this time the Japanese Red Army introduced the concept of 'kamikaze' attacks in acts of terrorist violence i.e., suicide bombings.

Beyond developing capacity to strike strategic targets, the PIRA developed increased tactical and technical proficiencies: in 1979 eighteen British soldiers were killed in a double remote IED detonation and gun battle at Warrenpoint that would today be referred to as a 'complex attack'. By 1987, the PIRA was proficient at systematically launching attacks on police bases with VBIEDs followed up by infantry assaults, a trend only belatedly limited by intelligence gathering and decisive military intervention. PIRA remained proficient at sourcing foreign support and supplies, and even as late as 1987 a weapons ship with over 150 tonnes of weapons and ordnance would be intercepted off Ireland[15].

The RAF were adept at fundraising through bank robberies, and also securing collaboration, not least through effective propaganda and 'branding', embodied in their 'Urban Guerrilla Concept' manifesto[16]. Even though all the first generation of RAF leaders were arrested and detained by June 1972, during their prolonged trial a second and third generation of RAF members were still able to seize the West German Embassy in Sweden in February 1975, assassinate a Federal Prosecutor (April 1977), murder the head of Dresdner Bank (July 1977), and intercept a convoy and kidnap the President of the German Employer's Association (September 1977).

Two developments in the Middle East were also of long-term significance. In 1983, members of the small 'Islamic Jihad' movement would conduct lethal suicide truck bombings against the UN-authorised Multinational Force in Lebanon, killing 241 US and 58 French military personnel in a single day. During the 1980s, Abdallah Azzam, a Palestinian cleric from a West Bank village, volunteered to fight in Afghanistan and subsequently played a crucial role in the internationalization of the jihadi movement by constructing the Maktab al-Khidamat (Afghan Services Bureau) with fellow volunteer Osama Bin Laden[17] to recruit Arabs and other volunteers to participate in the conflict.

Although the subsequent end of the Cold War – and the end of state sponsorship of terrorist groups by the Soviet bloc – was generally perceived as marking the end of terrorist campaigns, several attacks in the 1990s were a prelude for the wave of violence in the following decade, and indicated that the threshold of violence could be raised even higher than before. While new iterations of terrorist campaigns continued – ceasefires in Northern Ireland being preceded by mortar attacks on Downing Street at the height of the Gulf War, and later by truck bombs in the City of London – others indicated an expansion in terrorism's geographic scope. In 1993, a truck bombing was the first attempt to destroy the World Trade Centre in New York. The hijacking of an Air France jet in Algiers in 1994 reflected the ongoing terrorist capability to seize passenger jets. The same year, the Aum Shinrikyo cult conducted a small-scale sarin aerosol attack in Matsumoto, Japan, before, in 1995, provoking a mass casualty event by releasing sarin on three Tokyo metro lines killing 13 and injuring 6500 people. The 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City killed 168 people was the deadliest act of domestic terrorism in the history of the United States. Thereafter, in 1998 simultaneous explosions at US embassies in Kenya and Tanzania killed 224 and injured 4500, explosions that were soon linked to the Al-Qaeda network.

Of these attacks, the Christmas Eve 1994 Air France hijacking in Algiers was notable as the hijackers issued no demands, nor began hostage negotiations. Instead, the hijackers demanded to be allowed to fly to France, a demand only agreed to after three hostages were murdered. However, the plane had not been refuelled, and could only cross the Mediterranean to Marseille where a significant GIGN force assaulted the plane. In the aftermath, the French authorities revealed that the hijackers had intended to use the plane in a suicide attack on Paris[18]. The attack presaged a new era in which a G8 conference in Italy in July 2001 would already require air defences around the conference venue.

[15] See, Associated Press, 'Irishmen Charged in Seizure of Tons of Weapons', 5th November 1987, available at: https://apnews.com/article/b68cae02660499af1a766c27a4e46e60

[16] Available at: https://socialhistoryportal.org/sites/default/files/raf/en/0019710501%252520EN_2.pdf

[17] Thomas Hegghammer, *The Caravan: Abdallah Azzam and the Rise of Global Jihad*, (CUP: 2020).

[18] Peter Taylor, 'The Age of Terror', *BBC World* Service, May 2008 available at: https://www.bbc.co.uk/worldservice/documentaries/2008/05/080617_age_of_terror_three.shtml

Recruitment processes were also internationalising. Just as the Maktab al-Khidamat bureau had drawn international recruits to Afghanistan who continued to consolidate and expand operations thereafter under the umbrella of Al-Qaeda, in London the Finsbury Park mosque became a radicalisation hub, linking recruitment processes in Algeria, Chechnya, and Yemen, and sharing propaganda materials from each country[19].

2000s – 2020s

The Al-Qaeda operation to destroy the World Trade Centre in New York City is now well documented, although the failure to by domestic law enforcement services to act on intelligence of suspicious activity, to factor international intelligence sharing into decision making processes, and to maintain basic European security standards at airports created an environment ambitious terrorist networks were able to easily exploit.

During this period, states had to develop the capacity to address terrorist threats as the potential scale of attacks was perceived as larger than before, a reality reflected in the number of failed or disrupted plots against commercial aircraft, infrastructure, and mass-transit hubs. Well financed by generous donors, Al-Qaeda was able to encourage affiliates to mount bombing campaigns worldwide including Bali in 2002 (204 dead), Madrid in 2004 (191 dead), and London in 2005 (56 dead). Although volunteers could no longer travel to Afghanistan to meet high level Al-Qaeda personnel to plan and train for attacks as they had earlier, and as some volunteers moved to fight for in Iraq for Abu Musab al-Zarkawi's 'Al-Qaeda in the Land of the Two Rivers', the influence of Al-Qaeda's international networks still took nearly a decade to degrade.

However, the next phase of international terrorist violence drew on marginalised youth in Europe to achieve many of its ends. Four years after Al-Zarkawi's death, his associate Abu Bakr Al-Baghdadi became leader and rebranded the organisation as 'Islamic State of Iraq and the Levant' (IS), and rapidly expanded operations across Syria and Iraq, while separating from Al-Qaeda by 2013. Via its social media channels, IS began to actively solicit recruits from Europe and Asia to live in the extensive territories it controlled. Volunteers – including children – from Belgium, France Indonesia, Malaysia, North Caucasus, UK, and many other nations took commercial flights to Turkey and then easily moved across the border.

These volunteers and other sympathisers radicalised online mounted significant terrorist operations worldwide, with new attacks in Europe including attacks in Paris in January 2015 (12 dead) and November 2015 (137 dead), Brussels in March 2016 (35 dead), and Nice in July 2016 (87 dead). Crucially, IS affiliates proliferated beyond the Middle East, in the Caucasus, East Asia, Mozambique, Sahel, and West Africa. Their aggressive capacities have been reflected in the destruction of gas facilities and staff (Algeria and Mozambique), mass abductions of children (Nigeria), and the elimination of a US special forces unit (Niger).

In this environment, contemporary terrorists benefit from encrypted communications, extensive online audiences for propaganda, generous state sponsorship of Salafi/Wahhabi jihadist groups, and a lack of international capacity – and interest – to decisively intervene against IS affiliates with ground forces. Each new group builds on the foundations laid by their antecedents in the 1970s and 1980s until one or more states chooses to definitively disrupt and degrade terrorists' activities and capacities.

Contemporary Terrorism's Key Features – Organisational Strategies

Although somewhat underestimated until the later 1990s, effective and persistent terrorist groups have a strategic approach to a variety of operational challenges. This section outlines what may be termed terrorist groups' management strategies before addressing terrorists strategic objectives in the next section.

[19] See, for example, Jason Burke, 'All eyes on Britain as terror war accelerates', *The Observer*, 26th January 2003, available at: https://www.theguardian.com/uk/2003/jan/26/terrorism.immigrationpolicy

Military Strategy

Principally, detailed research in the 1990s demonstrated how the PIRA – perhaps unsurprisingly due to the long tradition of the IRA's Military Council – had a comprehensive military strategy that reflected the tensions between different members' ideology, politics, strategic communications, as well as the insecurity within the organisation created by counter-terrorist operations[20]. This strategy fed into the types of operations conducted and their frequency, as well as adaptation to facilitate bombing campaigns on the British mainland, increasingly implementing complex attacks in the mid-1980s on rural police stations after initial successes against Army convoys in the late 1970s, disrupting logistics chains and patrolling routes and formats, and targeting high-level political figures. The military strategy also adapted in response to military limiting a variety of operational activities in order to solely provide support to law enforcement services rather than taking on a variety of ´law enforcement activities for which they were neither trained nor equipped.

Technical Strategy

Secondly, any effective terrorist group will build in-house technical capacity to facilitate the planning and implementation of terrorist attacks. Training capacity on weapon systems, tactics, counter-surveillance, and IED placement has long existed alongside a skilled innovation capacity to create different types of bombs, shaped charges to defeat armour plating, and boobytraps. While this was seen with the PIRA campaigns in UK and Western Europe, the Islamic State have taken innovation to a new level with a dedicated budget and mass production lines for drone borne IED (DBIED) manufacture, a capacity developed alongside mass production of vehicle borne IEDs (VBIEDs)[21]. The considerable logistics challenges of sourcing and maintaining small arms and creating new explosive capabilities also require dedicated internal technical capacity, even if a terrorist group has state-level suppliers.

Fundraising Strategy

Thirdly, terrorists' approaches to fundraising are multi-faceted. Even with state sponsorship, groups are adept at soliciting external funds (Noraid in North America for the PIRA), generating their own funds by controlling smuggling and trafficking operations (diesel fuel and cigarettes for PIRA in Ireland, charcoal smuggling by Al Shabaab in Somalia), by extracting tax (or 'tribute') from a population (Al Shabaab in Somalia), or by bank robberies (Bolshevik 'expropriations' in Helsinki and Tbilisi[22], Red Army Faction in West Germany). However, although it is currently convenient to cite terrorist groups' entrepreneurial activities as an explanation for their funding sources, capability development, and overall growth via recruitment, the inconvenient reality is that state sponsorship has remained critical for the survival of key terrorist groups from the 1970s onwards, and for the expansion of terrorist groups into far broader revolutionary and state/emirate movements. Effective terrorist groups have always benefited from state support (PIRA from Libya, OIRA from Soviet Union, Red Army Faction from East Germany and the Soviet bloc), if not state direction. Some terrorist groups have benefit from significant private cash donations that are comparable to state-level support (Al Qaeda, Taliban, Lashkar-e-Taiba)[23].

Territorial Strategy

Terrorists will often seek to control territory, whether a street, a district, or a region. Whether express pol-

[20] M. L. R. Smith, *Fighting for Ireland? The Military Strategy of the Irish Republican Movement*, Routledge, 1995.

[21] For a general overview of all the technological avenues open to terrorist groups see, for example, Afzal Ashraf and Anastasia Filippidou, *Terrorism and Technology*, NATO Centre of Excellence Defence Against Terrorism, 2017, available at: https://www.tmmm.tsk.tr/research.html

[22] It is interesting to note that the New York Times' contemporary account of the Bolshevik bank robbery in Tbilisi in 1907 refers to 'terrorists' rather than 'bank robbers'. See: https://www.nytimes.com/1907/06/27/archives/bomb-kills-many-170000-captured-missile-thrown-by-terrorists-at-a.html

[23] See, for example, 'Wikileaks: Saudis 'chief funders of Sunni militants'', *BBC News*, 5th December 2010, available at: https://www.bbc.com/news/world-middle-east-11923176

icy – such as the Islamic State implementing their version of Sharia law in the former Emirate – or an exercise in demonstrating control of a space – as with the continued use of ‘punishment beatings’ or ‘kneecapping’ against youth drug dealers and other petty criminals in Northern Ireland – terrorists can establish themselves as the *de facto* authorities where they are unchallenged. As with some criminal groups, similar levels of control can be affected in prisons. Sometimes control of a building or buildings is sufficient to create an unregulated space in which radicalisation and planning can be conducted in one or more countries as occurred at London’s Finsbury Park Mosque. The areas controlled by some terrorist groups may be small but the control reinforces the lack of government access to provide a variety of services and to enforce the law. Any space in which terrorists are not subject to surveillance – whether Afghanistan, Syria, or training camps in the Middle East in the 1970s – facilitates an acceleration of terrorist capacities.

Communications Strategy

These approaches feed into remaining strategic elements of communications and recruitment. Terrorist groups have proved adept at creating propaganda, whether through pamphleteering (the Red Army Faction’s ‘Urban Guerrilla Concept’), campaigns for political status of prisoners (PIRA’s 1981 Hunger Strike), or simply the image of what PIRA and their political wing Sinn Fein referred to as ‘spectaculars’: enormous bombs destroying infrastructure with no military value, whether landmark buildings or commercial centres. Terrorist groups can also exploit any overreaction by the state for propaganda purposes, whether the deaths of civilians in protests, torture inhumane or degrading treatment in custody, or detention without trial.

In terms of simple and persistent imagery, terrorist groups’ murals across Northern Ireland remain and are now tourist attractions[24]. Nevertheless, violent imagery has always been a central element of terrorist activities since the 1970s: whether the aftermath of assassinations of public officials, kidnappings, destruction of passenger aircraft, or destroyed vehicles. But images of many types of aggressive violence are now dominant across terrorists’ communication and social media channels, and – whether interpreted as raw propaganda or strategic messaging to solicit sympathisers to join and actively participate in a struggle – feeds directly into recruitment processes.

Recruitment Strategy

In terms of recruitment, sometimes – particularly at the start of a terrorist movement – amongst any marginalised, disempowered, disenfranchised, or unemployed group it can be easier for terrorists to acquire volunteers. The actions of the state can accelerate this process. A variety of ties, whether those of community, family, ethnicity, or religion can drive recruitment. Usually such ties are local or regional, but can also incorporate some sympathisers at capital and international level.

But today, online radicalisation targeted has secured a much wider international audience and potential recruitment pool, particularly across young people using social media. Considerable time and resources go into online recruitment and messaging to target vulnerable groups and individuals and to cultivate not only their grievances but also their ambitions. An overlooked dimension of contemporary radicalisation is that some IS recruits have material as well as psychological motivations: female British recruits would highlight the material benefits of being widowed when a spouse was ‘martyred’[25]. The success of online recruiters is reflected in 3000-5000 EU citizens travelling to Syria by January 2015[26], and 10000 citizens from OSCE states travelling to Syria by 2017[27].

[24] Rachel Hall, ‘‘Troubles Tourism’: Should Derry be celebrating its political murals?’, *The Guardian*, 12th August 2019, available at: https://www.theguardian.com/cities/2019/aug/12/troubles-tourism-should-derry-be-celebrating-its-political-murals

[25] Nabeelah Jaffer, ‘The secret world of Isis brides: 'U dnt hav 2 pay 4 ANYTHING if u r wife of a martyr'’, *The Guardian*, 24th June 2015, available at: https://www.theguardian.com/world/2015/jun/24/isis-brides-secret-world-jihad-western-women-syria

[26] Piotr Bakowski and Laura Puccio, ‘Briefing: ‘Foreign Fighters’ – Member States’ responses to EU action in an international context, European Parliamentary Research Service, February 2015, available at: https://www.europarl.europa.eu/EPRS/EPRS-Briefing-548980-Foreign-fighters-FINAL.pdf

[27] See, for example, United States Mission to the OSCE, ‘Response to OSCE Chairperson-in-Office Sebastian Kurz, Special Representative of the Chairperson-in-Office on Countering Radicalization and Violent Extremism Professor Peter Neumann, and OSCE Secretary General Thomas Greminger, As delivered by Acting Deputy Chief of Mission Michele Siders to the

Terrorist groups also screen those they have recruited as not all recruits have the same skillsets: recruited by the then military chief of AQ Mohamed Atef, the ringleader of the 9/11 attacks Mohammed Atta was introduced to Osama Bin Laden in Afghanistan in 1999. Bin Laden and Atef knew they had a recruit capable of managing a large-scale operation and immediately sent Atta on to meet the 9/11 plot's organiser Khalid Sheikh Mohammed in Karachi. Mass online recruitment now offers effective terrorist groups the chance to build momentum and diversify skillsets across an organisation much more quickly than twenty years ago.

Online radicalisation has also led to the emergence of spontaneous individual or small cells of terrorists, the disruptive effects of which can be seen in stabbings, shootings, vehicle-ramming attacks, and bombings such as the Manchester Arena attack in 2017. Although some more complicated plots still involve face-to-face meetings between groups and recruits, current right wing Neo Nazi recruitment feeds into similar feelings of alienation and disenchantment, with an Australian terrorist using online extremist forums as inspiration for the attack on two mosques in New Zealand in 2019.

Contemporary Terrorism's Strategic Objectives

Historically, most terrorist movements have had a national focus, with occasional alliances of convenience between different geographical terrorist cells to seek common goals and share technical expertise. With the emergence of Al Qaida, and later the Islamic State and its self-proclaimed franchises and affiliates[28], there was a realisation that some terrorist groups now aspire to a global reach far more quickly than was previously considered possible.

In addressing contemporary terrorists' various strategic objectives, and to address the appropriate counter terrorist strategies of states themselves, it is possible to concisely summarise their broad features – both of challenges and responses – in terms of 'strategic terrorism', a format in which terrorists seek to aggressively accelerate their campaigns to create a critical mass of awareness and support in order to achieve their goals. This contemporary aspiration is built on the tried and tested methods of previous terrorist campaigns.

Contemporary 'Strategic Terrorism' can be defined as an effort by groups which employ terrorism as the main plank of their strategy – 'strategic terrorists' – to bypass both the mass agitation and military elements of guerrilla and revolutionary warfare theory, in the belief that the use of symbolic violence alone – and its saturation of mass media – will be sufficient to achieve desired political objectives[29].

Terrorists' operational objectives evolve in three stages: **disorientation**; **target response**; **gaining legitimacy**. The objective of **disorientation** is to alienate the authorities from their citizens, reducing the government to impotence in the eyes of the population, which will be perceived as unable to cope with a situation of evolving chaos.

Secondly, in terms of **target response**, the objective is to induce a government to respond in a manner that is favourable to the insurgent cause, principally by provoking the government into actions that are illegal or regarded as repressive overreactions that destroy the political middle-ground.

Permanent Council, Vienna', 29th September 2017, p. 2., available at: https://www.osce.org/files/f/documents/a/d/351106.pdf

[28] On the rapid and ongoing development of IS franchises, see, for example, Patrick Tucker, 'Mozambique Is Emerging As The Next Islamic Extremist Hotspot', *Defense One*, 6th July 2020, available at: https://www.defenseone.com/threats/2020/07/mozambique-emerging-next-islamic-extremist-hotspot/166638/ For the joint threat still posed by AQ and IS in the franchise context see, for example, Colin Clarke and Jacob Zenn, 'ISIS and Al-Qaeda's Sub-Saharan Affiliates Are Poised for Growth in 2021', *Defense One*, 26th February 2021, available at: https://www.defenseone.com/ideas/2021/02/isis-and-al-qaedas-sub-saharan-affiliates-are-poised-growth-2021/172313/

[29] Neumann and Smith, 'Strategic Terrorism', p. 576.

Thirdly, to gain **legitimacy** with alienated or disaffected social, ethnic, or religious groups, terrorists seek to exploit the emotional impact of the violence to insert an alternative political message and seek to broaden a support, often through the media or political front organizations[30]. In this way, push and pull factors are exploited by terrorists to drive recruitment.

This is the context in which this handbook places domestic and international terrorist threats. The following chapters address the nature of an effective state – and whole-of-society – response to these threats.

[30] Neumann and Smith, ‘Strategic Terrorism’, p. 590.

Chapter Two: Challenges of counterterrorism in a democratic state

Introduction

> *Combating and ultimately overcoming terrorism will not succeed if the means to secure that society are not consistent with human rights standards ... Such an approach does not call for the balancing of liberty and security or suggest that liberty, or aspects of it, must be sacrificed to achieve security ... Counter-terrorism tactics that do not comply with human rights law may ultimately be declared unlawful, resulting in failed prosecutions or overturned convictions. Counter-terrorism tools that do not comply with human rights are therefore liable to be ineffective*[31].

Democracies, by virtue of being open societies, are automatically vulnerable to many types of terrorist activity. Inevitably, terrorism imposes particular challenges on democratic states, not least how to deter, manage, and limit the risk of terrorism, but also to define an appropriate democratic response to all types of terrorist activities.

In seeking to develop the capacity to prevent and combat terrorism and violent extremism, democratic states need to go beyond building capacity in relation to the provision of security by law enforcement, security services, or the armed forces. Instead, to ensure maximum effectiveness when preventing and countering terrorism, states need to address the broad policy, strategic, and legislative frameworks for countering terrorism, specify the roles and tasks of a broad range of government ministries and agencies, and adopt a whole-of-government and whole-of-society approach to prevention.

This final step comprises establishing a broad, inclusive network of stakeholders and practitioners to coordinate a range of counter-terrorism and P/CVE programmes. In short, as with any other security challenge they face, societies need to adopt a multi-dimensional approach to counter-terrorism and P/CVE. This chapter outlines key best practices democracies can adopt to address the multiple challenges of counter-terrorism and C/PVE.

Terrorism and the Democratic State – Vulnerabilities and Opportunities

States are inherently vulnerable to terrorist groups – or terrorist recruiters – for the simple reason that democratic freedoms of speech, movement, association, and privacy can all be exploited by terrorist groups as much as they are already exploited by domestic and international criminal networks. This situation is now exacerbated by extensive low-cost international travel networks, lax visa regimes at some travel hubs, and the proliferation of encrypted communications, particularly via mobile apps. States also need to anticipate terrorists' technological innovations and retain sufficient capacity to prevent security failures.

States face a simple dilemma. If a state is inactive, or simply passive, in the face of a terrorist threat, terrorists can rapidly exploit a variety of social, political, and economic spaces for their own benefit, and keep expanding until a state responds. At the same time, states are particularly vulnerable if they over-react to a terrorist threat: treatment of suspects, detention without trial, lack of legal process, unwarranted interception of communications, censorship, and marginalisation of social or ethnic groups can lead to an aggressively negative reaction not only from a group or groups perceiving themselves as a target or victim of government policy, but also from sympathisers across the wider society. Instead of using existing powers and resources at their disposal and to manage their strategic approach to terrorism, states'

[31] OSCE ODIHR, *Countering Terrorism, Protecting Human Rights*, 2008, p. 20.

overreaction often leads to the creation of duplicative – and controversial – powers and capacities in response to threats.

Keeping in mind the key features of ‘Strategic Terrorism’, terrorists often seek to precipitate a negative response amongst the general public to state policy and practice, disrupt, and disorient the state and society, and, in so doing, gain legitimacy with one or more segments of society. States need to be prepared to prevent terrorists achieving their intended outcomes.

Any government, particularly in European democracies, is also vulnerable in terms of legal jeopardy: any breach of regional norms or conventions or treaties can have legal as well as political repercussions, as well as an obligation to pay compensation, if standards are not upheld. In some worst-case scenarios, a lack of legality in one country can disrupt information and intelligence sharing between democracies as, for example, evidence obtained through illegal acts such as torture is inadmissible in court.

Vulnerabilities - States’ Overreaction to Terrorist Threats

States’ overreactions to terrorist threats have similar features that are now well documented. By avoiding these bad practices, states have an immediate opportunity to ensure the credibility and legitimacy of their counter terrorist and C/PVE programming.

In responding to terrorist threats, some states have adopted measures that have unlawfully denied freedom of expression, freedom of assembly and freedom of association, cumulatively resulting in the criminalisation of protest, the suppression of public debate, and public anger at the use of repressive measures. Sometimes asylum and refugee law and practice have been particularly affected, with individuals being illegally deported and refugee claims being improperly considered. Racial profiling has also been used in discriminatory ways. The cumulative result of such measures has not led to a reduction of the terrorist threat, but rather exacerbated long-standing grievances, as well as undermining the values of democracy, the rule of law, and civil society[32].

In particular, the case law of domestic courts, international courts and tribunals, and the work of UN mechanisms, documents how some counter-terrorism measures have resulted in:

- detention, sometimes for protracted periods, without charge;
- denial of the right to challenge the lawfulness of detention;
- denial of access to legal representation;
- monitoring of privileged conversations with legal counsel;
- secret incommunicado detention; and ill-treatment, even torture, of detainees as well as inhumane and degrading conditions of detention;
- abduction (sometimes referred to as rendition) to another country.

It is important to note that the involvement of European states in rendition processes has also led to the payment of significant damages to victims once liability was established through legal process[33].

[32] See OSCE, *Countering Terrorism, Protecting Human Rights*, pp. 20-21.

[33] See, for example, the case of Libyan national Abdul Hakim Belhaj who received a formal apology from the UK government, but waived the right to compensation, and whose wife received compensation as she was pregnant when renditioned with her husband. ‘Belhaj rendition: UK apology over Libyan dissident treatment’, *BBC News,* 10th May 2018, available at: https://www.bbc.com/news/uk-44070304. The British government would ultimately spend GBP 11m resisting demands for an apology, compensation, and prosecutions of government personnel, with GBP 4.4m spent on government lawyers, and GBP 6.9m to cover all of Abdul Belhaj’s legal costs. Owen Boycott, ‘UK spent GBP 11m of public money fighting Libya rendition case’, *The Guardian*, 25th April 2019, available at: https://www.theguardian.com/world/2019/apr/24/uk-public-money-fighting-libya-rendition-case-abdel-hakim-belhaj-fatima-boudchar

In a context where the use of force by police or any other security provider can be divisive at local community level, as well as in other contexts such as protests, any contentious act by one or more security sector personnel can ultimately render the state vulnerable to repercussions at national and international levels. As the state's overall response to terrorist threats will impact the level of grievance and define the public perceptions of the state's credibility, states must carefully calculate the proportionality of their response to terrorism. Calibrating the broad range of state counter terrorist policies and practices is essentially a function of managing risk through oversight, training, and education.

Vulnerabilities – Limited Oversight of Security, Counter-Terrorist, and P/CVE Policy

In Europe, the lack of effective oversight of counter-terrorist and P/CVE policies by democratic institutions, civil society, and the media has also been linked to a broader overreaction to terrorist threats. For example, at the national level, despite measured responses to terrorism in the 1980s and mid-1990s, France has more recently been accused of abandoning its secular foundations to build an 'anti-terrorist republic', an argument framed in terms of a collective lack of oversight:

> The shift in the French approach has been particularly evident over the last twenty years and it has taken place outside any democratic process. Public opinion has not found sufficient material to form a sure and reasoned opinion on anti-terrorist policy, neither in the media — which are primarily interested in the audience violence attracts — nor in parliamentary debates, due to a lack of knowledge and interest on the part of elected representatives. In fact, this shift has crept slowly, often hidden behind the emotions and grandstand effects that usually followed the attacks[34].

This particular vulnerability, also evident in other democracies, can be remedied by effective multi-stakeholder oversight frameworks that will be addressed in the following sections.

Opportunities – Contemporary P/CVE and Counter-Terrorism Best Practice

Democracies benefit from a situation in which much of the foundational work on counter-terrorism guidance has already been completed. For example, long form guidance on 'The International Framework to Combat Terrorism' remains valid for orienting new staff and stakeholders on P/CVE and counter-terrorism issues[35], with subsequent chapters addressing the challenges a state faces in protecting human rights in a counter-terrorist context.

The more recent International Centre for the Study of Radicalisation (ICSR) policy paper / Austrian OSCE Chairmanship-in-Office report on P/CVE pulls together a variety of issues and standards affecting the OSCE area and simply outlines best practice across each thematic area[36], including National Action Plans, Prisons, Policing, Youth, Education, Religion, The Internet, Women, Refugees, Interventions, and Returnees.

States now adopt a strategic approach to P/CVE and counter-terrorism, with policy documents consolidating both a whole-of-government and whole-of society approach to P/CVE issues. The guidance of the Council of Europe is a useful reference point to develop a strategic consensus around three priorities to:

[34] Francois Thuillier, 'A Strange War', *AboutIntel.eu*, 27th July 2020, available at: https://aboutintel.eu/france-anti-terrorist-republic/

[35] See, 'Chapter 4: The International Framework to Combat Terrorism: An Overview', in OSCE ODIHR, *Countering Terrorism, Protecting Human Rights: A Manual*, 2008, pp. 34-42, available at: https://www.osce.org/odihr/29103

[36] The same paper is available in two formats with slightly different pagination: Peter Neumann, 'Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region', OSCE, CIO.GAL/189/17, (September 2017) p. 38, available at: https://www.osce.org/chairmanship/346841 ; and as Peter Neumann, 'Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region', *ICSR*, September 2017, https://icsr.info/2017/09/29/release-director-peter-neumanns-osce-report/

Prevent terrorism: through criminal law and law enforcement measures aimed at disrupting attacks or their preparation and through multifaceted longer-term measures aimed at preventing radicalisation, including countering recruitment, training, the dissemination of terrorist ideology and the financing of terrorism;

Prosecute terrorists: ensuring that terrorist offences committed in Europe or abroad are investigated in the most efficient and quickest possible manner, also through effective judicial and international co-operation and that those responsible are brought to justice and answer for their acts, in respect of human rights and the rule of law;

Protect all persons present on the territories of the member States against terrorism, providing for the security of the people and the protection of potential targets of terrorist attacks, including critical infrastructures and public spaces; provide assistance, and offer support to victims of terrorism[37].

Beyond this simple strategic approach of **prevention**, **prosecution**, and **protection**, the fundamental challenge states face is to successfully implement and adapt best practice across government and the security sector. Beyond orientation, the triple challenge of training, coordination, and implementation is that of organising government and society's counter-terrorism focal points. The coherence of the counter terrorist and P/CVE will depend on the ability of government focal points to lead multiple stakeholders in the same direction. The availability of specific P/CVE guidance for governments, law enforcement, security services, and civil society is helpful to address this significant challenge. Integrating these challenges into a government's strategic approach to P/CVE can maximise the positive impact of P/CVE programming. Relevant materials are used throughout this handbook and subsequent chapters to maximise the opportunities for successful P/CVE programming.

The next section outlines broad remedies for the vulnerabilities faced when democracies develop a strategic approach to counter-terrorism and C/PVE. The following sections then outline further solutions that also inform successful institutional approaches to P/CVE, some of which are also outlined in greater detail in the subsequent chapters.

Policy and Legal Challenges

Human Rights and Counter-Terrorism

A simple way to address the issue of democracies and counter-terrorism in general, and policy and legal challenges in particular, is to simply do so from the perspective of protecting human rights i.e., protecting citizens and society. It is important to note that this approach is relevant across all Council of Europe member states in which the policy and practice of national security - from community to strategic levels - is determined by the European Convention on Human Rights which remains binding upon all signatories[38]. And that the UN Special Rapporteur 'on the promotion and protection of human rights and fundamental freedoms while countering terrorism' has advocated for the same approach[39].

[37] Council of Europe Counter-Terrorism Strategy (2018-2022), available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808afc96

[38] For background material on the impact of ECHR on national security issues, see, for example, Iain Cameron, *National Security and the European Convention on Human Rights*, (Uppsala: Uppsala University, 2000); and Iain Cameron, 'National Security and the European Convention on Human Rights – Trends and Patterns', in *Stockholm International Symposium on National Security and the European Convention on Human Rights*, (Stockholm: Commission on Security and Integrity Protection, 2008).

[39] Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Ten areas of best practices in countering terrorism', *Human Rights Council*, A/HRC/16/51, 22nd December 2010 available (with updated technical guidance) at: https://www.ohchr.org/en/issues/terrorism/pages/annual.aspx

By placing the positive obligation of human rights protection at the heart of policy it is easier to explain, develop, and legitimise a whole-of-government and whole-of-society approach to preventing extremism and countering terrorism. The same standards are also those that a state should integrate into existing security policy and practice, not only at the level of strategic security policy, but also in the legislative framework for policy implementation, and the relevant guidance developed by government institutions and security providers for personnel working at public-facing levels.

All states have an obligation to provide their citizens with protection against a variety of threats including terrorism. Human rights standards impose positive obligations on states to ensure the right to life, protection from torture, privacy, right to liberty and safety, and to a fair trial. In short, any act of terrorism infringes on all the rights that it is a state's positive duty to protect.

This does not mean that an act of terrorism should automatically be considered an absolute failure to protect citizens. However, if a democratic state fails to take adequate and appropriate measures to protect citizens' rights, the state itself bears some responsibility for the violation. Therefore, developing an effective counter-terrorism strategy can be considered a part of a state's overall human rights obligations, as an element of the state's fundamental role to protect citizens, as well as a strategic policy document for government ministries, security providers, and related government agencies.

In developing strategic guidance, the Council of Europe's 'Guidelines on Human Rights and the Fight against Terrorism' are relevant as they reconcile legitimate national security concerns with the protection of fundamental freedoms and states' duty to protect human rights. Beyond the positive obligations, the exhaustive seventeen guidelines specify the need for:

- prohibition on arbitrariness and discrimination;
- prohibition on torture;
- regulation of surveillance;
- right to due process;
- prohibition on the death penalty;
- provision for surveillance of detainee's communications with legal representatives[40].

In following this guidance, states can avoid legal and political vulnerabilities inherent in malpractice as well as ineffective implementation. Consequently, these human rights standards are directly relevant to the development of counter-terrorism and P/CVE strategies, and preventing and breaking the cycle of grievances driving violent extremism. In parallel, they are also directly relevant to the development of broader security policies and practices. The next section outlines how existing policy development, monitoring, and oversight processes can integrate counter-terrorism and P/CVE issues and approaches.

Democratic Oversight of Security, Counter-Terrorism and P/CVE Policy

As a now a well-established European and international principle, democratic oversight of the security sector remains vital to ensure transparency and accountability of – and thus public trust in – all security policy and practice[41]. With an overall rationale that prioritises public safety, responsive security policies

[40] Council of Europe, 'Guidelines of the Committee of Ministers of the Council of Europe on human rights and the fight against terrorism adopted by the Committee of Ministers on 11 July 2002 at the 804th meeting of the Ministers' Deputies', pp. 35-38, available at: https://edoc.coe.int/en/terrorism/7544-protection-of-victims-of-terrorist-acts.html. Also see the 'Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism', CETS No. 217, 2017, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217

[41] See, for example, in Eden Cole, Philipp Fluri, and Simon Lunn (eds.), *Oversight and Guidance: Parliaments and Security Governance*, (DCAF & NATO PA: 2015), available at: https://www.academia.edu/20827428/Oversight_and_Guidance_Parliaments_and_Security_Sector_Governance

and practices, effective resource management[42], and the key attributes of good governance[43], this expansive oversight framework offers a simple means of ensuring that counter-terrorism and P/CVE best practice can be wholly integrated into broader security policy and practice, and offers an established framework to approach P/CVE issues.

The oversight process can also serve as a catalyst for enhancing cooperation – and building confidence between - between democratic institutions (principally parliament), broader government agencies, civil society, and the media. Establishing broad consultancy mechanisms and feedback loops, much in the same way as community policing policy and practice benefits from feedback via plurality of community policing boards, as well as parliamentary input via security, policing, human rights, and other legislative committees. This oversight format can thus be used for intensive development – or simply adaptation – and implementation of counter-terrorism and C/PVE policy, practice, and legislation.

Nevertheless, there is still a need to develop specialised oversight capacity on certain counter terrorist and P/CVE issues. One practical example is the UK's establishment of a specific post of the 'Independent Reviewer of Terrorist Legislation' in the 1970s, with the selected barrister reporting to both parliament and the government during their term in office. Another key element of the post is dealing with the media, legal community, and civil society organisations. Although not an uncontroversial responsibility, the continued requirement for clear guidance has ensured that the Reviewer continues their work to this day[44]. More generally, the UN's 2005 establishment of a 'Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' position reflected the need for global guidance that could be integrated into global policy and practice on an ongoing basis[45]. Subsequent sections and chapters outline in more detail how stakeholders can work together on key oversight and P/CVE policy issues in a constructive and dynamic format.

Breaking the Cycle of Grievance & Recruitment

Breaking the cycle of grievances within one or more societal groups – the key driver of extremist recruitment – is vital to limit the influence of any terrorist network. In order to do this, states need to ensure that policy and practice are in line with best practice, that frontline personnel are fully trained and oriented, and that any action taken to counter and prevent terrorism is legitimate, proportionate, necessary, and non-discriminatory[46].

This simple approach prioritises human rights protection in order to ensure public safety. By limiting the interference with one or more rights, the scope for antagonising a particular segment of society is automatically limited. Nevertheless, the simplicity of the approach relies on a democratic society's tolerance, pluralism, and broad-mindedness, all of which enable the fair treatment of minorities.

Preventing grievance in day-to-day service provision

In practical terms, governments need to ensure everyday life for the wider society and groups at high risk of radicalisation features equal access to services and protection from security threats. This general requirement presupposes that citizens can equally access a variety of socio-economic services including administrative, housing, medical, justice, and education services. Inherent in this requirement is that citizens have equal access to security provision, principally through law enforcement services. This broad approach disrupts push and pull factors driving violent extremism.

[42] Eden Cole, 'Democratic Oversight of Defence and Security Institutions', in Cole, Fluri, Lunn (eds.), *Oversight and Guidance*, p. 44-45.

[43] 'The role of good governance in the promotion of human rights', UNCHR Res. 2000/64, UN Doc. E/CN.4/RES/2000/64, p. 277. Available at: http://www.un.org/en/terrorism/pdfs/2/G0014048.pdf

[44] https://www.gov.uk/government/organisations/independent-reviewer-of-terrorism-legislation

[45] See reports of the Special Rapporteur at https://www.ohchr.org/en/issues/terrorism/pages/annual.aspx

[46] See OSCE ODIHR, *Countering Terrorism, Protecting Human Rights*, pp. 68-70 & p. 80.

From this baseline, government and the security sector can implement proportionate measures to counter extremist activities. Historically, one of the largest drivers of grievances, beyond a lack of access to general services, were detention without trial, and harassment and arbitrary violence inflicted by security sector personnel. Extensive guidance exists to limit the risk of provoking grievance, whether for law enforcement in their day-to-day activities[47], or when conducting investigations[48], or for intelligence professionals monitoring terrorist activities and communications[49]. More broadly, guidance on breaking the cycle of grievance is already integrated into civil society[50] and whole-of-society approaches to preventing extremism[51]. Another element relevant to grievance is education: although this is usually seen in terms of preventing online radicalisation, ensuring access to education also offers both an opportunity for accessing other services more efficiently, foster a positive sense of identity and belonging[52], and to strengthen the rule of law[53].

Victims of Terrorism

When thinking about grievance, democracies also need to protect victims of terrorism. In the Council of Europe context, the 'Revised Guidelines on the Protection of Victims of Terrorist Acts'[54] address a range of issues affecting victims including the need for emergency assistance, investigation and prosecution, effective access to the law and to justice, administration of justice, and compensation[55]. Similarly, the EU's legislation on the standing of victims in criminal proceedings equally applies to the victims of terrorist acts. The legislation is binding on EU member states and deals with issues such as compensation, access to courts, and protection of witnesses. Notably, the legislation also covers victims who are not residents of a state where a terrorist incident occurred[56].

Breaking the Cycle of Recruitment – Wider Society

The measures outlined in the previous section on breaking the cycle of grievance are relevant to breaking the cycle of recruitment. Ensuring no sections of society are excluded from access to services, and that the provision of public security does not alienate individuals or groups, remains vital to prevent disaffected individuals joining radicalised groups in the first instance. Repeated violations of individual rights can create a critical mass of extremist sympathisers – including individuals who feel insecure due to a lack of reliable public security – and lead to an irrevocable breach between state and citizens. At the same

[47] OSCE and OSCE ODIHR, *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach*, 2014, available at: https://www.osce.org/secretariat/111438

[48] OSCE and OSCE ODIHR, *Human Rights in Counter-Terrorism Investigations, A Practical Manual for Law Enforcement Officers*, 2013, available at: https://www.osce.org/odihr/108930

[49] Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, Human Rights Council, A/HRC/14/46, 17th May 2010, available at: https://www.ohchr.org/EN/Issues/Terrorism/Pgages/Issues.aspx. Also see: Aidan Wills, 'Democratic and effective oversight of national security services', Council of Europe, *Issue Paper*, May 2015, available at: https://rm.coe.int/1680487770

[50] OSCE, *The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Guidebook for South-Eastern Europe*, August 2018, available at: https://www.osce.org/files/f/documents/2/2/400241_1.pdf

[51] OSCE, *A Whole-of-Society Approach to Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism - A Guidebook for Central Asia*, January 2020, available at: https://polis.osce.org/wholeofsociety-approach-preventing-and-countering-violent-extremism-and-radicalization-lead

[52] See, UNESCO, 'Strengthening the Rule of Law through Education: a guide for policymakers, UNESCO: 2017, p. 12, available at: https://unesdoc.unesco.org/ark:/48223/pf0000247764

[53] See, for example, UNESCO, 'Strengthening the Rule of Law through Education', and other materials available at: https://en.unesco.org/themes/gced/rule-law

[54] Council of Europe, 'Revised Guidelines of the Committee of Ministers of the Council of Europe on the protection of victims of terrorist acts adopted by the Committee of Ministers at its 127th Session, Nicosia, 19 May 2017', pp. 5-10, available at: https://edoc.coe.int/en/terrorism/7544-protection-of-victims-of-terrorist-acts.html

[55] OSCE, *Countering Terrorism, Protecting Human* Rights, p. 28.

[56] EU Council Framework Decision of 15 March 2001 on the standing of victims in criminal proceedings (2001/220/JHA), OJ L 082/1, 22/03/01, pp. 1-4.

time, government and civil society need to disrupt and combat terrorist recruitment narratives, not least through creating counter narratives which emphasise the human cost of terrorist activities.

Breaking the Cycle of Recruitment – Radicalisation in Prisons

Penitentiary systems are now high-risk locations for radicalisation. Prison management need to ensure that prisoners – even those deemed at low risk of radicalisation – are not exposed to recruitment by individuals convicted of terrorist offences, whether acts of violence or supplying support for terrorist groups.

Maintaining good prison standards, wherein custodial practices respect human rights and prevent grievances, is a vital first step to ensure radicalisation prevention[57]. A variety of management strategies are available to manage specific radicalisation risks, including dispersing prisoners convicted of terrorist offences, or concentrating them in one facility, and rehabilitating former extremists. Tools such as assessment and classification systems for identifying 'at risk' prisoners can also be used to prevent radicalisation of the prison population [58], as well as training prison staff to identify the adoption of violent extremist behaviour. Staff also need to ensure that terrorist offenders are neither supporting terrorist networks outside detention facilities, nor themselves receiving support from those networks[59].

Breaking the Cycle of Recruitment – Non -custodial rehabilitation and reintegration

To avoid the possibility of radicalisation in prison settings, guidance has also been developed on rehabilitation and reintegration programmes outside prisons, including roles for non-government actors[60]. The rise in terrorism prosecutions has led to an increase in the number of individuals associated with violent extremism serving prison sentences, many of whom will eventually be released into a community, typically at a relatively young age. Instead, multi-actor rehabilitation and reintegration initiatives can play a role in minimising terrorism-related recidivism. Such initiatives can also manage the growing number of individuals, often women and children, returning from conflict zones in Iraq and Syria who may have been radicalised by violence or the families they have grown up in.

Breaking the Cycle of Recruitment – Youth Radicalisation

The last decade of recruitment by IS has shown that Western European youth are particularly vulnerable to recruitment. This not only includes schools but also online 'grooming' and recruitment through social media channels. Detecting, monitoring, and disrupting these channels is vital to prevent radicalisation. Moreover, education and access to reliable information is one step towards creating 'digital citizens' who can easily identify disinformation and extremist propaganda. Additional material on education follows in Chapter Four and in the section below on 'Detection and Monitoring'.

[57] See short form guidance at: Council of Europe, *Guidelines for prison and probation services regarding radicalisation and violent extremism*, 2nd March 2016, pp. 2-3, available at: https://rm.coe.int/16806f3d51 ; and Council of Europe, *Council of Europe Handbook for Prison and Probation Services Regarding Radicalisation and Violent* Extremism, 1st December 2016, available at: https://rm.coe.int/16806f9aa9

[58] Penal Reform International, Preventing Radicalisation in Prisons: Developing a Coordinated and Effective Response, December 2015, p. 4., available at: https://cdn.penalreform.org/wp-content/uploads/2016/02/PRI-Radicalisation-briefing-paper-V2.pdf

[59] Radicalisation Awareness Network, 'Dealing with radicalisation in a prison and probation context, RAN Working Group on Prison & Probation', Practitioners Working Paper, 2018, available at: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-papers/archive/ran-pp-practitioners-working-paper_en

[60] OSCE, *Non-custodial Rehabilitation and Reintegration in Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Guidebook for Policymakers and Practitioners in South-Eastern Europe*, January 2020, available at:
https://polis.osce.org/noncustodial-rehabilitation-and-reintegration-preventing-and-countering-violent-extremism-and

Protection Challenges

As outlined in the 'Policy and Legal Challenges' section, all states face expansive protection challenges. The key to solving this challenge is an active and comprehensive approach to preventing breaches of human rights across society in general, while prioritising efforts to protect individuals and societal groups at risk of radicalisation in particular.

The bulk of the protection task already lies with government and its frontline services providers, and, in the context of public security, with law enforcement agencies. In terms of protection, it is also important to emphasise that citizens need access to an independent and capacitated justice system that is responsive to the needs of citizens. However, specialised capacity is required in the context of counter-terrorism and P/CVE. The key to protection against extremism is to identify vulnerable groups in society, and to focus on those most at risk of radicalisation, particularly youth.

Analysing strengths and weaknesses to identify gaps in security provision, and to identify vulnerabilities across society, whether in relation to vulnerable socio-economic or ethnic groups, or structural weaknesses in service provision or monitoring capacities, or technical and infrastructural weaknesses, can be a first step to formulating relevant prevention policies and capacity development needs in a comprehensive strategic document. Additionally, governments need to look beyond vulnerabilities at the local and national levels and identify similar risks at the regional and international levels.

Identifying additional resources to complement those already available is crucial, and the process of solving or managing protection challenges is also integral to the following sections on 'Resource Management' and 'Disinformation' issues.

Resource Management and Capability Challenges

State and society face considerable resource management and capacity challenges when tacking P/CVE, but the challenge is essentially one of developing a coherent policy, strategy, and capacity, and then ensuring coherent implementation. Where feasible, many government employees can essentially pursue a dual function, addressing terrorism in the same way that they would address a basket of criminal risk issues, service delivery, and public security challenges that they face in the line of their daily work.

Nevertheless, creating dedicated capabilities to monitor, prevent, investigate, and to counter terrorist threats requires the establishment and maintenance of a core group for all national counter-terrorism and C/PVE programming. This core then provides the framework for all whole-of-government, institutional, and whole-of-society counter-terrorism and C/PVE programming that integrates existing practitioners and stakeholders dealing with broad portfolio of public security issues. Once such a broad group exists, the challenge is to establish current awareness, coordination, and training frameworks to maintain its capacity. This section outlines specific C/PVE skills and capacities requiring dedicated human and financial resources.

Legal and Policy Capacity

Reviewing legislation to ensure it is consistent with human rights standards is a constant task. Although government professionals – and legal experts in wider education and civil society – provide input in line with their professional background, retaining a small core of dedicated counter-terrorism and P/CVE legal and policy expertise to draw on national and international best practice is a necessity as a nation adapts to changing threats.

Detection and Monitoring – Radicalisation Narratives and Recruitment Activity

State and society need to monitor a variety of social groups and media to detect radicalisation processes. At the community level of 'everyday' monitoring, law enforcement, educators, and community groups need to watch for signs of radicalisation activities or extremist propaganda or any other activities. This approach ensures accessibility and visibility on the part of service providers who need to be seen by and accessible to local communities. In parallel, such accessibility counters any sense of 'alienation' from broader society, or of an area's control by organisations other than government institutions.

New forms of passive and non-intrusive online monitoring are also available. As social media channels are instrumentalised for terrorist recruitment, opportunities exist to automatically detect 'hate speech' used in radicalisation processes, with some methods already having over 80% accuracy[61]. As of May 2016, several technology companies that play an unintended but significant role in the proliferation of hate speech, including Facebook, Google, Microsoft, and Twitter, have jointly agreed to a European Union Code of Conduct to remove illegal online hate speech within 24 hours[62]. A related Terrorist Content Analytics Platform (TCAP)[63] promotes tech companies in tackling use of the internet by terrorists, and the Global Internet Forum to Counter Terrorism provides broad guidance on developing trends[64].

One more recent development from which counter-terrorist and P/CVE professionals can benefit is the proliferation of open-source investigation organisations and specialists who monitor a variety of social media channels for information on new developments in conflict zones. Although these include some focused on state activity[65], some individuals comprehensively monitor radicalisation and extremist networks in real time[66].

Some countries have introduced monitoring programmes in the education sphere, but tailoring these effectively is important and, essentially, no different to monitoring other types of potentially anti-social or criminal behaviour. The issue is addressed further in Chapter Four.

Detection and Monitoring – Criminal Activity

Monitoring is already a significant component of the investigations branch of law enforcement agencies responsible for detecting criminal activity. Illicit trafficking of firearms, fuel, narcotics, cigarettes, counterfeit goods, and cultural objects, as well as trafficking in human beings, racketeering and extortion have become lucrative ways for terrorist groups to obtain funding. By monitoring such activities, law enforcement can already flag a variety of extremist activities to counter terrorist authorities.

Detection and Monitoring – Surveillance and Interception of Communications and Bulk Data

In terms of more intrusive monitoring related to suspicions of individuals' involvement in terrorism, any surveillance component needs to be in line with best practice outlined in the previous policy and legal challenges section. The necessity for any interception of communications needs to be evidence based, proportionate, and time-limited, remains constant. Ensuring the legitimacy of any intercept is vital for

[61] Tom De Smedt, Guy de Pauw, and Pieter Van Ostaeyen, 'Automatic Detection of Online Jihadist Hate Speech', *Computational Linguistics & Psycholinguistics CliPS Technical Report Series*, CTRS 007, February 2018, available at: https://www.academia.edu/36127816/Automatic_Detection_of_Online_Jihadist_Hate_Speech

[62] Alex Hern, 'Facebook, YouTube, Twitter and Microsoft sign EU hate speech code', *The Guardian*, 31st May 2016, https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code

[63] https://www.terrorismanalytics.org/about

[64] https://gifct.org/

[65] See, for example, https://www.bellingcat.com and https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/.

[66] See, for example, https://twitter.com/p_vanostaeyen, and https://twitter.com/ajaltamimi.

any counter-terrorist prosecutions, as will be detailed in a following section below. At the same time, there is a need for technical and human surveillance capacities, some of which can be provided by existing investigations branches of law enforcement, but additional capacity may be required for dedicated counter-terrorist investigations. As a broad guide, the initiative 'about:intel' at the non-profit Stiftung Neue Verantwortung collates a range of contemporary guidance on surveillance law, whether bulk collection of data, or interception of communications[67].

Analytical Capacity

Drawing together the detection and monitoring challenges listed above, states need the capacity to accumulate and analyse information on extremist activity. Existing capacity can be used to log and flag terrorist relevant information, but dedicated analysts are required to interpret and assess the information in the context of broader – often classified – information shared by international partners, as well as information gained from authorised interception of communications. National 'fusion centres' can perform a critical role in aggregating the data from across government that is needed to enable the development of all-source threat assessments that inform policy and practice in a timely fashion[68].

Analytical capacity needs to have a predictive element. States need to anticipate terrorists' strategic and technological innovations in order to prevent security failures, and to retain the capacity to prevent and defeat new innovations. Terrorists' innovations are often predictable[69] and measures need to be developed to protect against and defeat new weapon and explosive systems. The current weaponisation of small drone technology, using cheap 'off the shelf' components, requires the creation of measures to defeat such devices in a variety of contexts.

Coordination Capacities

The need for additional coordination capability on CT and P/CVE issues exists at three levels: Firstly, the need for a national 'fusion centre' that draws on the existing monitoring capacities of across security sector agencies. Secondly, the need for a whole-of-government and whole-of-society group that pools professionals and stakeholders from across society, service providers, and the security sector to review policy and practice and share information on extremist activities. Thirdly, designated government and security sector focal points need the capacity to formally interact with their peers at the international level, sharing information and analysing information received from third parties.

Evidence Collection

Some terrorism prosecutions require long term evidence collation, and additional forensic capacity may be required to secure minute pieces of evidence from a crime scene and to test the evidence in certified laboratories. Similarly, additional surveillance capacity may be required to legally intercept communications at national and international levels. Ensuring a capacity do this beyond those already in place for law enforcement and investigations units is a key resource management issue for any government.

[67] See https://aboutintel.eu/

[68] Belgian Standing Committee I, *Fusion Centres Throughout Europe: All-Source Threat Assessments in the Fight Against Terrorism*, (Intersentia, 2010). See also, for example, Renske van der Veer, Walle Bos, Liesbeth van der Heide, 'Fusion Centres in Six European Countries: Emergence, Roles and Challenges', *ICCT Report Series*, February 2019, available at: https://icct.nl/app/uploads/2019/02/ICCT-VanderVeer-Bos-VanderHeide-Fusion-Centres-in-Six-European-Countries.pdf

[69] Andrew Silke and Anastasia Filippidou, 'What drives terrorist innovation? Lessons from Black September and Munich 1972', *Security Journal*, Volume 33, June 2020, pp. 210-227, available at: https://dspace.lib.cranfield.ac.uk/handle/1826/14221

Prosecution

One of the most significant challenges for any state is outlining an appropriate legal framework for prosecuting terrorists or their facilitators. Ensuring the existing criminal code reflects the European best practice outlined in the 'Policy and Legal Challenges' section allows for a more expansive approach to prosecuting terrorist supporters as well as active terrorists themselves.

As per the previous section on evidence collection, having the capacity to gather evidence in a systematic and warranted way to meet a credible threshold of proof is vital to ensure the likelihood of securing a conviction against a suspect, and for detaining suspects in a first instance. This comprehensive approach also helps limit the risks of illegitimate actions that drive terrorist recruitment, principally the arbitrary detention and unsafe prosecutions of terrorist suspects. The positive momentum of credible prosecutions helps address the push and pull factors of radicalisation, breaking the cycle of grievance, and other drivers of terrorism such as lack of access to services.

Human and Financial Resources

The above list has detailed how existing – and budgeted – capacities can be used to develop and share information, alongside the need for a core group of anti-terrorist professionals. Existing law enforcement, investigation, and intelligence capacity limit the cost of counter-terrorism and C/PVE capacity. By using these existing resources , it is easier to cost the need for additional core capacity and coordination frameworks. Some surplus capacity may also be required to handle a surge in threats, but drawing on a reserve of professionals previously working in the sector is one way to address this requirement and limit costs.

Information and Disinformation Challenges

Addressing information and disinformation challenges in a society comprises the need to ensure the availability of reliable information, that policy objectives are clear, that practices are uncontroversial, that disinformation narratives are challenged, and that government reacts to crises with reliable information.

The principal element of addressing both information and disinformation challenges is to ensure the national media sector is independent and shares reliable information. A well-capacitated media, reflecting balance and depth in reporting, enhances public trust and confidence in news sources. Independent regulators are one means of achieving this goal.

Similarly, governments need to ensure that reliable information is shared with the media. This requirement is fundamental to ensure confidence in information. Any unreliable information quickly degrades trust in government.

Governments also need to be proactive in their communication, particularly strategic communications. By identifying the nature of a terrorist threats, outlining the types of risks, and clearly elaborating the government's strategic response to terrorism can all create confidence in a government's proactive approach to addressing the problem. Any ambiguity or lack of communication creates an information vacuum in which public trust is quickly degraded.

Government needs to proactively identify and flag disinformation. By monitoring sources of disinformation or radicalisation narratives, particularly on social media channels, governments have an early opportunity to flag disinformation and formulate a public response that disrupts the channels' effectiveness. Another element of this proactive government approach is to liaise with focal points at global web platforms. While some platforms do engage in crisis management with state representatives to shut down broadcasts and livestreams by terrorists in real time, platforms have later struggled to remove footage, and some non-EU and non-North American platforms continue to allow unredacted propaganda and war crime footage.

At the same time, governments need to avoid allegations of arbitrary censorship. Striking an appropriate balance can be difficult in extreme circumstances, but this challenge is essentially the same as in any other crisis management situation. Some remedies exist, such as time limited censorship may be necessary in highly limited circumstances. But censorship often backfires on governments, especially amongst terrorist sympathisers. Instead, the effectiveness of a counter-terrorism strategy in general and P/CVE communications in particular will negate any immediate need to adopt severe draconian censorship measures.

Chapter Three: Institutional Frameworks

Introduction

To ensure the safety of their citizens, all democratic states require a comprehensive institutional approach to counter-terrorism and preventing violent extremism. The long-term effectiveness of any P/CVE strategy is improved by a whole-of-government and whole-of-society approach in which institutions not only systematically perform their specified roles but also dynamically cooperate with other stakeholders to achieve a nation's intended outcomes.

To achieve this objective, a clear strategic framework for counter-terrorism and P/CVE needs to be developed, collective and individual institutional goals need to be specified, institutional capabilities need to be built and maintained, and sufficient resources need to be attributed to counter-terrorism and P/CVE -specific capabilities.

This chapter focuses on institutional frameworks for addressing P/CVE issues, addressing the overall approach to developing policy and then focusing on institutions' individual challenges and requirements. Mapping the design elements of a substantive policy centred on the institutions, the chapter addresses the requirements of putting policy into practice, effective cooperation formats, and the particular challenges facing individual institutions in monitoring, countering, and disrupting extremist activities.

Legal Dimensions

The established European legal framework for counter-terrorism and P/CVE provides the context for developing relevant policy strategies, implementation frameworks, and other remedies. As per the earlier guidance in Chapter 1 and Chapter 2, the legal dimensions overviewed here feed directly into the formulation of policy guidance for institutions.

These legal standards are the same as those that a state should integrate into existing security policy and practice, not only at the level of strategic security policy, but also in both the legislative framework for policy implementation and the guidance developed by government institutions and security providers for personnel working at public-facing levels. The key to developing successful guidance is to identify and specify counter-terrorism and P/CVE challenges in relevant policies so that the majority of practitioners can orient themselves and then adapt their approach from broader security provision issues to P/CVE programming.

European Definitions – Prevention Objectives

The European legal framework for counter-terrorism and P/CVE clearly defines, in a harmonised fashion, the activities that comprise terrorism, all of which must be addressed by policy and practice. Intentional criminal acts – including murder, kidnapping, hijacking, infrastructure attacks, and threats to commit any such acts – must be considered as terrorist acts if they have any of the following objectives:

- to seriously intimidate a population; or
- to unduly compel a government or international organization to perform or abstain from performing any act; or
- to seriously destabilise or destroy the fundamental structures of a country or an international or-

ganisation[70].

The rapid evolution of terrorist threats over the last decade has led to the inclusion of additional intentional acts such as:

- the travel and return of 'Foreign Terrorist Fighters', principally citizens;
- various types of terrorist financing and illicit trafficking;
- the role of intermediaries in supplying services to terrorist groups;
- posting online content;
- soliciting terrorist offences;
- the provision of training for the purposes of terrorism;
- and recruitment for the purposes of terrorism[71].

States must address the emergence of *ad hoc* extremist cells alongside more well-established terror groups, a "terrorist group" can be of limited size and limited time duration, namely:

> 'a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences'[72] ... 'that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure[73]'.

Per the 2005 Council of Europe Convention on the Prevention of Terrorism, states also need to be ready to extradite, collect evidence, and/or prosecute in relation to terrorist offences[74]. Consequently, the C/PVE agenda focuses on prevention of a broad range of possible extremist offences.

Human Rights and Counter-Terrorism – Protection Obligations

In terms of all security policy and practice, all states have an obligation to provide their citizens and societies with protection against a variety of threats including terrorism. Human rights standards impose positive obligations on states to ensure the right to life, protection from torture, privacy, right to liberty and safety, and to a fair trial. Any act of terrorism infringes on the rights that it is a state's positive duty to protect. As a result, preventing violent extremism contributes to protecting as wide a segment of society as possible, not least through minimising the risk of terrorist activities.

Across all Council of Europe member states, the policy and practice of national security – from community to strategic levels – is determined by the European Convention on Human Rights which remains binding upon all signatories[75]. Approaching counter-terrorism legal and policy challenges from the perspective

[70] EU Council Framework Decision of 13 June 2002 on combating terrorism, (2002/475/JHA), OJ L 164, 22/06/2002, Art. 1(1), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002F0475

[71] Directive (EU) 2017/541 of the European Parliament and of the Council of 15th March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Articles 8-19, available at: http://data.europa.eu/eli/dir/2017/541/oj and https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A32017L0541

[72] EU Council Framework Decision of 13 June 2002 on combating terrorism, Article 1.

[73] EU Council Framework Decision of 13 June 2002 on combating terrorism, Article 2.

[74] Council of Europe, 'Convention on the Prevention of Terrorism', *CETS*, No. 196, Article 15 and Articles 17-21, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196

[75] For background material on the impact of ECHR on national security issues, see, for example, Iain Cameron, *National Security and the European Convention on Human Rights*, (Uppsala: Uppsala University, 2000); and Iain Cameron, 'National Security and the European Convention on Human Rights – Trends and Patterns', in *Stockholm International Symposium on National Security and the European Convention on Human Rights*, (Stockholm: Commission on Security and Integrity Protection,

of protecting human rights, strategic and operational policy guidance must reconcile legitimate national security concerns with the protection of fundamental freedoms and rights. To this end, states must :

- prohibit arbitrariness and discrimination;
- prohibit torture;
- regulate surveillance;
- ensure the right to due process;
- prohibit the death penalty;
- prohibit surveillance of detainee's communications with legal representatives[76].

In an institutional context, there is also a need to follow best practice related to retaining personal information per the terms and conditions of the Global Data Protection Regulation (GDPR)[77].

These legal obligations shape the prevention agenda by ensuring that best practice is central to all types of counter-terrorist and P/CVE interventions. Stakeholders involved in prevention activities must maintain high standards in their programming and daily activities to avoid provoking any grievances. In following this guidance, and incorporating into strategic and institutional strategies, states can avoid legal and political vulnerabilities inherent to any malpractice and ensure more credible and legitimate practices: this challenge is addressed in the next section.

Policy Dimensions

The established policy framework for P/CVE seeks to disrupt and prevent extremism by disrupting extremists' operational objectives. States require a hierarchy of policy documents to ensure a precise focus on whole-of-society P/CVE activities, and the next sections highlight best practice to achieve state and society's preferred P/CVE objectives.

Core Priorities

In adopting a strategic approach to P/CVE and counter-terrorism, policy documents can consolidate both a whole-of-government and whole-of society approach to P/CVE issues. In order to ensure credible and legitimate practices, and to disrupt terrorists' operational objectives of **disorientation**; **target response**; and **gaining legitimacy,** and to disrupt the **pull and push factors** that drive broader radicalisation. The guidance of the Council of Europe is a reference point for developing a strategic consensus around three core priorities to:

> **Prevent** terrorism**:** through criminal law and law enforcement measures aimed at disrupting attacks or their preparation and through multifaceted longer-term measures aimed at preventing radicalisation, including countering recruitment, training, the dissemination of terrorist ideology and the financing of terrorism;

2008). The UN Special Rapporteur 'on the promotion and protection of human rights and fundamental freedoms while countering terrorism' has advocated for the same approach: Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Ten areas of best practices in countering terrorism', *Human Rights Council*, A/HRC/16/51, 22nd December 2010 available (with updated technical guidance) at: https://www.ohchr.org/en/issues/terrorism/pages/annual.aspx

[76] Council of Europe, 'Guidelines of the Committee of Ministers of the Council of Europe on human rights and the fight against terrorism adopted by the Committee of Ministers on 11 July 2002 at the 804th meeting of the Ministers' Deputies', pp. 35-38, available at: https://edoc.coe.int/en/terrorism/7544-protection-of-victims-of-terrorist-acts.html. Also see the 'Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism', CETS No. 217, 2017, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217

[77] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Prosecute terrorists: ensuring that terrorist offences committed in Europe or abroad are investigated in the most efficient and quickest possible manner, also through effective judicial and international co-operation and that those responsible are brought to justice and answer for their acts, in respect of human rights and the rule of law;

Protect all persons present on the territories of the member States against terrorism, providing for the security of the people and the protection of potential targets of terrorist attacks, including critical infrastructures and public spaces; provide assistance, and offer support to victims of terrorism[78].

This simple strategic approach of **prevention**, **prosecution**, and **protection** enables institutions and stakeholders across wider society to orient themselves on their shared role in P/CVE, and to incorporate best practices into their programming interventions. The key national challenge is to organise and coordinate government and society's P/CVE focal points to achieve these three objectives.

The coherence of any counter terrorist and P/CVE programming is dependent on the ability of government focal points to lead multiple stakeholders in the same direction through cooperation and coordination frameworks. The availability of specific P/CVE guidance for government institutions, law enforcement, security services, and civil society is also crucial to address this significant challenge. At the same time, states need to go beyond building capacity in relation to public security provision by the security sector, and to ensure other stakeholders have sufficient skills, resources, and cooperation frameworks to address programming and cooperation challenges.

Policy Hierarchy – P/CVE from National to Local Levels

P/CVE policy proceeds from a comprehensive set of national policy documents. A **National Security Policy / Strategic Security Policy** document specifies threats and challenges and both the policy and resource allocation response to those threats.

In the context of the National Security Policy (NSP) document, a national **Counter Terrorism Strategy** outlines specific terrorist threats and the policy response at national level, and specifies the responsibilities and roles of government agencies implementing policy.

Proceeding from the NSP and Counter-Terrorism Strategy, the final requisite document is an expansive **National P/CVE Strategy and Action Plan** which outlines the extent of radicalisation threats and drivers and specifies the policy response of a broad range of societal stakeholders, going beyond government and its agencies to local government, education, and civil society.

P/CVE Action Plans are valuable as their rationale is to tightly define and focus a broad range of prevention activities and create a common societal understanding of multiple stakeholders' responsibilities in countering extremism[79]. The **UN Action Plan** published in late 2015 remains a useful reference point for developing a comprehensive approach to radicalisation prevention. Designed to complement national counter-terrorism strategies where they already exist, the Plan's focuses on the need to disrupt local and national drivers of violent extremism. The push and pull factors driving extremism are categorised as:

- Lack of socio-economic opportunities;
- Marginalisation and discrimination;

[78] Council of Europe Counter-Terrorism Strategy (2018-2022), available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808afc96

[79] Peter Neumann, 'Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region', OSCE, CIO.GAL/189/17, (September 2017), pp. 45-46, available at: https://www.osce.org/chairmanship/346841

- Poor governance, violations of human rights and of the rule of law;
- Prolonged and unresolved conflicts;
- Radicalisation in prisons;
- Individual background and motivation;
- Collective grievances and victimisation;
- Distortion and misuse of beliefs, political ideologies and ethnic and cultural differences;
- Leadership and social networks, including new communication media[80].

The seven thematic areas for disrupting the drivers are categorised as:

- Dialogue and Conflict Prevention,
- Strengthening Good Governance,
- Human Rights and the Rule of Law,
- Engaging Communities,
- Empowering Youth,
- Gender Equality and Empowering Women,
- Education,
- Skill development and Employment Facilitation,
- Strategic Communications, the Internet, and Social Media[81]

Although less than half of OSCE participating States had created such a national action plan by 2016, the template serves as a useful precedent and provides the framework for a number of National Action Plans currently in force[82]. For example, Switzerland's '**National Action Plan to Prevent and Counter Radicalisation and Violent Extremism**' proceeds from the basis of the UN Action Plan[83] and outlines, in detail, a variety of best practices.

The Swiss Action Plan serves as a template for understanding whole-of-government and whole-of-society approaches to preventing violent extremism. The plan factors in earlier national guidance, including the **Counter-Terrorism Strategy**[84], the **Federal Intelligence Service's 2017 Annual Report's** finding that jihadist-motivated radicalisation constitutes the main threat to Swiss society[85], the **Foreign Policy Action Plan on PVE**[86], the reports of a dedicated multi-agency **Terrorist Tracking Task Force** (TETRA)[87],

[80] Report of the Secretary General, 'Plan of Action to Prevent Violent Extremism', A/70/674, 24th December 2015, pp. 7-10, available at: https://www.un.org/counterterrorism/plan-of-action-to-prevent-violent-extremism and https://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674

[81] Report of the Secretary General, 'Plan of Action to Prevent Violent Extremism', pp. 14-20. For additional guidance on developing National Action Plans, see Also see Hedayah Center, 'Guidelines and Good Practices: Developing National P/CVE Strategies and Action Plans', September 2016; available at: https://www.hedayahcenter.org/resources/good-practices/guidelines-good-practices-developing-national-p-cve-strategies-action-plans/ and ICCT, '12 Principles for National Action Planning', International Center for Counter-Terrorism, 30th June 2016; available at https://icct.nl/update/12-principles-for-national-action-planning/

[82] Neumann, 'Countering Violent Extremism', pp.45-46.

[83] Swiss Security Network (Sicherheitsverbund Schweiz), *Swiss National Action Plan to Prevent and Counter Radicalisation and Violent Extremism*, 4th December 2017, available at: https://www.newsd.admin.ch/newsd/message/attachments/50703.pdf pp. 5-6.

[84] *Strategie der Schweiz zur Terrorismusbekämpfung [Switzerland's Counter Terrorism Strategy]*, BBI 2015 7487, 18th September 2015, available in DE/FR/IT only at: https://www.fedlex.admin.ch/de/fga/index/2015 and https://www.fedlex.admin.ch/eli/fga/2015/1784/de

[85] Federal Intelligence Service (2017). *Sicherheit Schweiz – Lagebericht 2017 des Nachrichtendienstes des Bundes [Swiss Security – 2017 Report of the Federal Intelligence Service]*, available at: https://www.newsd.admin.ch/newsd/message/attachments/48133.pdf

[86] FDFA, *Switzerland's Foreign Policy Action Plan on Preventing Violent Extremism*, 2016, available at: https://www.eda.admin.ch/eda/en/fdfa/fdfa/publikationen/alle-publikationen.html/content/publikationen/en/eda/schweizer-aussenpolitik/Aussenpolitischer-Aktionsplan-PVE160404

[87] The TETRA Task Force is headed by the Federal Police and includes the Federal Intelligence Service, Office of the Attorney General, Foreign Affairs, Border Guard, State Secretariat for Migration, Federal Office of Justice, the Conference of Cantonal Police, and the National Police Command. For an overview, see: https://www.fedpol.admin.ch/fedpol/en/home/terrorismus/terrorismus-aktuelle-lage/schweiz-ist-aktiv.html

and the first national report on **money laundering and terrorist financing risks**[88]. Based on the UN Plan, the plan outlines preventive measures adapted for Switzerland's confederal structure that aim to curb enabling (push) factors and influencing (pull) factors driving extremism[89].

The Plan's four goals are simple, aiming to create 'practicable pre-conditions for preventing and countering radicalisation and violent extremism in all its forms', while – in line with the policy and legal guidance outlined in this section and earlier chapters – at the same time 'respecting fundamental and human rights'[90], through:

- Cooperation and effective structures
- Coordination
- Instruments
- Inclusion and Support of Civil Society[91]

The multi-dimensional approach of the Swiss Action Plan incorporates many institutions and a focus extending to the community and local level, with the plan being formulated at federal and cantonal level by directors of **Social Services**, directors of **Education**, the association of **communes** and the union of **cities**, as well as **Justice** and **Police** directors[92]. The inclusive – and necessarily expansive – approach is immediately emphasised in the first 'cooperation' goal of the plan: as the strategy is 'developed at local level (canton, region, city) and supported at a political level'[93], it defines the networks of relevant stakeholders and the common course of action in C/PVE, the Plan recommends:

> ... that **school authorities**, **social services**, **social** and **youth workers**, **child and adult protection authorities**, **psychiatric services**, **police**, **intelligence services** (depending on the context at federal or cantonal level), **cantonal and juvenile prosecution services**, **integration agencies** and **other specialist agencies** be involved as well as those in the immediate environment of the person [at risk of radicalisation] concerned, depending on the situation[94].

In this way, the plan seeks to identify problematic developments and potential risks of extremism and violence as early as possible and to initiate suitable preventative measures across state institutions and wider society. The activity areas and series of operational measures elaborated in the Action Plan are addressed in the next section.

[88] See: State Secretariat for International Finance (SIF), 'First national report on money laundering and terrorist financing risks', 19th June 2015, available at: https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-57750.html, Also see, Swiss Confederation, 'Report on the risks of money laundering and terrorism financing in the case of non-profit organisations - Report by the interdepartmental coordinating group on combating money laundering and the financing of terrorism', 28th June 2017, available at: https://www.newsd.admin.ch/newsd/message/attachments/48921.pdf. Also see the later National Risk Assessment (NRA) on the 'Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding', published as: Swiss Confederation, 'National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding - Report of the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF)', October 2018, available at https://www.sif.admin.ch/dam/sif/en/dokumente/Integrität des Finanzplatzes/nra-bericht-krypto-assets-und-crowdfunding.pdf.download.pdf

[89] *Swiss National Action Plan*, p. 6.

[90] *Swiss National Action Plan*, p. 10.

[91] *Swiss National Action Plan*, p. 10.

[92] *Swiss National Action Plan*, p. 5.

[93] *Swiss National Action Plan*, p. 10.

[94] *Swiss National Action Plan*, p. 10.

Operational Dimensions

To implement P/CVE strategies effectively, a broad cooperation and coordination structure is required to pull together the prevention work of multiple institutions across society. Creating such a structure in line with best practice also ensures greater political responsibility for preventing extremism from national to local levels. Implementing C/PVE strategies requires proactive measures by designated parties, and having a clear cooperation framework ensures clarity on responsibilities, information sharing, and can also build greater momentum towards early prevention interventions.

Government Services

As discussed in Chapters 1 and 2, a lack of access to services can drive grievances that lead to extremism. Ensuring frontline service providers, across health, social, housing, and education, identify ways to provide straightforward access in areas at risk of extremism, and identifying requisite operational capacity to achieve that, is a first step to managing the risk of extremism.

Security Providers

In their day-to-day operations, activities, investigations, security providers have to avoid negative behaviour that provoke grievances and drive extremism. As with other service providers, security institutions have to be accessible to the public in general, especially in areas at risk of radicalisation. More importantly, security providers – principally community police – also need to build trust and cooperative relationships with the general public, with information gained through these relationships feeding back into radicalisation monitoring platforms and processes.

Abundant operational guidance for security providers relates to both general operational conduct, including guidelines on the use of force[95] and minimum standards for the treatment of prisoners[96], and P/CVE-specific issues facing: public-facing law enforcement services[97]; intelligence/security services[98]; penitentiaries[99]; and the criminal justice sector[100].

At the operational level, for security providers a fusion centre is the key structure for effective counter-terrorism coordination and action, principally to handle real-time information from different institutional sources at national and international levels for deliberate or immediate action[101]. To implement a P/CVE

[95] UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, 1990, available at: https://www.ohchr.org/en/professionalinterest/pages/useofforceandfirearms.aspx

[96] UN Standard Minimum Rules for the Treatment of Prisoners ('the Mandela Rules'), 2015, available at: https://www.unodc.org/documents/justice-and-prison-reform/Nelson_Mandela_Rules-E-ebook.pdf

[97] OSCE and OSCE ODIHR, *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach*, 2014, available at: https://www.osce.org/secretariat/111438

[98] Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, Human Rights Council, A/HRC/14/46, 17th May 2010, available at:
https://www.ohchr.org/EN/Issues/Terrorism/Pgages/Issues.aspx. Also see: Aidan Wills, 'Democratic and effective oversight of national security services', Council of Europe, *Issue Paper*, May 2015, available at: https://rm.coe.int/1680487770 . Also see: Global Counterterrorism Forum, 'Recommendations for Using and Protecting Intelligence Information in Rule of Law -Based, Criminal Justice Sector-Led Investigations and Prosecutions', GCTF: 2016, available at:
https://toolkit.thegctf.org/en/Resources/Articles/Detail/id/69

[99] Council of Europe, *Handbook for Prison and Probation Services Regarding Radicalisation and Violent Extremism,* PC-CP, December 2016, available at: https://rm.coe.int/16806f9aa9

[100] UNODC, *Handbook on Criminal Justice Responses to Terrorism*, UNODC Criminal Justice Handbook Series, 2009, available at:
https://www.unodc.org/documents/terrorism/Handbook_on_Criminal_Justice_Responses_to_Terrorism_en.pdf

[101] Belgian Standing Committee on Control of Intelligence and Security Services, *Fusion Centres Throughout Europe:*

action plan effectively, there is a need for a wider coordination network structure to be in place as a format to manage a whole-of-society approach to monitoring, detecting and preventing violent extremism.

Whole-of-Society P/CVE Coordination Network

To consolidate a national P/CVE approach, a whole-of-society coordination network offers a structure in which multiple institutions and stakeholders can work towards common prevention goals.

Taking the Swiss Action Plan as an example, its expansive approach includes **school authorities**, **social services**, **social** and **youth workers**, **child and adult protection authorities**, **psychiatric services**, **police**, **intelligence services** (depending on the context at federal or cantonal level), **cantonal and juvenile prosecution services**, **integration agencies** and **other specialist agencies**[102].

Similarly, the expansive scope and broad institutional responsibilities of the Norway's C/PVE Action Plan are reflected at the outset in a Foreword text signed off by ten government ministers: **Justice and Public Security**; **Labour and Social Affairs**; **Foreign Affairs**; **Culture**; **Local Government and Modernisation**; **Children, Equality and Social Inclusion**; **Defence**; **Education and Research**; **Health and Care Services**; and the **Prime Minister**[103].

To achieve four national prevention goals, the Swiss network works across five thematic activity areas with twenty-six specific measures for the specified stakeholders to address. The activity areas condense the guidance in the UN Action Plan into:

- Knowledge and Expertise (nine measures)
- Cooperation and Coordination (eight measures)
- Prevention of extremist ideologies and extremist groups (three measures)
- Disengagement and reintegration (four measures)
- International Cooperation (two measures)

The plan specifies the roles and tasks of institutions and other stakeholders, such as youth groups and charities, to implement each measure from national to local level, identifies service providers and users[104], and outlines political responsibility for each measure and funding sources for each action[105].

The Swiss Action Plan also foresees future developments to improve coordination including the formal creation of a **National Coordination Office** (Measure 16[106]) and cantonal '**Competence and Advice Centres**' focused on C/PVE issues in general and performing an **early warning** function in particular (Measure 10[107]). In this way, the Action Plan not only itemises institutions' roles and responsibilities but also foresees the creation of more advanced and even more highly structured C/PVE capabilities.

All-Source Threat Assessments in the Fight Against Terrorism, 2010. Also see, for example, Renske van der Veer, Walle Bos, Liesbeth van der Heide, 'Fusion Centres in Six European Countries: Emergence, Roles and Challenges', *ICCT Report Series*, February 2019, available at: https://icct.nl/app/uploads/2019/02/ICCT-VanderVeer-Bos-VanderHeide-Fusion-Centres-in-Six-European-Countries.pdf

[102] *Swiss National Action Plan*, p. 10.

[103] Norwegian Ministry of Justice and Public Security, 'Action Plan against Radicalisation and Violent Extremism", 28th August 2014, p. 5, available at: https://www.regjeringen.no/en/dokumenter/Action-plan-against-Radicalisation-and-Violent-Extremism/id762413/

[104] 'Annex', *Swiss National Action Plan*, pp. 31-32.

[105] 'Masterplan', *Swiss National Action Plan*, pp. 27-29. In the case of the Norwegian Action Plan, the responsibility for each measure is attributed to a particular ministry only. See, Norwegian Ministry of Justice and Public Security, 'Action Plan against Radicalisation and Violent Extremism', p. 3.

[106] *Swiss National Action Plan*, p. 18.

[107] *Swiss National Action Plan*, p. 16.

Resource Management Dimensions

The costs of many P/CVE-relevant institutional capabilities and requirements are already incorporated into national and institutional budgets. The human and financial resources required for front-line staff and infrastructure to provide basic services across a country should already be incorporated into a national budget. However, counter-terrorist and P/CVE taskings may require dedicated budgets for additional training, monitoring, coordination, and operational activities.

In the security sector, the requirement to fund front-line law enforcement activities would typically already be covered by a significant component of an Interior Ministry's share of the national budget, just as, in parallel, a Justice Ministry's budget covers the provision of judicial services and the judiciary itself. The bulk of intelligence and security services' personnel and equipment costs should similarly be already 'priced in' to their budget allocation. In a broader institutional context, ministries providing other public services, whether health, social, or housing, should similarly have a minimum budget to provide public-facing personnel and maintain infrastructure.

Resource management challenges specific to P/CVE can be seen in the requirement to develop P/CVE -specific capacities across all institutions, as well as other societal stakeholders, and to ensure coordination of P/CVE activities. This requirement usually includes P/CVE training for all stakeholders, but may also require dedicated human and financial resources to ensure a network of focal points is in place to address P/CVE issues, and to develop and maintain brand new P/CVE-specific capacities and platforms such as a national P/CVE coordination framework. Ultimately, the amount of additional financial requirement is dependent on the terrorist threat level and radicalisation risks – the more prevention is successful, the lower the minimum financial allocation for these P/CVE-specific capacities will be in the long run.

Attributing additional resources to meet new P/CVE challenges is a political decision, and linking requirements to both existing and new budgets is crucial to ensure both the transparency and efficiency of the process. In the case of Switzerland, each measure specified in the C/PVE Action Plan is attributed to a specific budget[108], or – if the plan acknowledges that additional resources may be required for a particular purpose – identifies the future legislative and budgetary context for those resources to be supplied.

For example, the Swiss Action Plan sometimes emphasises that training institutions need to supply relevant content and services out of their existing budget[109], or that particular threat management activities draw on an established budget line[110]. In limited instances recourse to private foundations is recommended, but the national research budget is also noted as available to support certain P/CVE research activities[111]. However, in other instances, the Swiss Action Plan foresees that new resources will be required and indicates the plan for securing them:

> A framework ordinance, based on Article 386 of the Swiss Criminal Code (SCC), is planned in order to regulate future crime prevention at federal level, so that the federal government can provide financial support in this field for projects in civil society to prevent and counter radicalisation and violent extremism[112].

The plan also notes instances in which no additional funds are required for a particular activity[113].

[108] *Swiss National Action Plan*, pp. 27-29.

[109] For example, 'Measure 4: Training of support workers in the federal centres and the cantonal centres for asylum seekers', and 'Measure 5: Raising awareness among and providing training for key people', *Swiss National Action Plan*, p. 15.

[110] 'Measure 14: Development and introduction of the concept of threat management', *Swiss National Action Plan*, p. 17.

[111] 'Measure 1: Organising research projects and studies on radicalisation and violent extremism in Switzerland', *Swiss National Action Plan*, p. 13.

[112] *Swiss National Action Plan*, p. 9.

[113] 'Measure 15: Regulation of the exchange of information between authorities', *Swiss National Action Plan*, pp. 17-18.

In conclusion, the additional resources required for P/CVE-relevant and P/CVE-specific measures at institutional and societal levels can be identified through a thorough assessment of a terrorist threat, and then exhaustively itemised in a National Action Plan. Sourcing additional resources for a national coordination network can be placed in the context of crime prevention, but burden sharing – and maximising the contribution of existing training and information sharing networks – offers an opportunity to optimise the management of resources. The challenge each nation faces is to reach a political consensus on the total number of measures required to prevent extremism and to match adequate resources to those requirements.

Chapter Four: Radicalisation Prevention

> *There is no evidence that shows a single path or one single event which draws a young person to the scourge of extremism: every case is different. Identifying people at risk of being radicalised and then attracted to extremist behaviour is very challenging. It also makes the task of countering extreme views complex and difficult. If the Government adopts a broad-brush approach, which fails to take account of the complexities, and of the gaps in existing knowledge and understanding of the factors contributing to radicalisation, that would be counter-productive and fuel the attraction of the extremist narrative rather than dampening it.*
>
> *House of Commons Home Affairs Committee, 'Radicalisation: the counter-narrative and identifying the tipping point', Eighth Report of Session 2016–17, HC 135*[114]*.*

Introduction

The European Commission simply defines radicalisation as:

> ...a phased and complex process in which an individual or a group embraces a radical ideology or belief that accepts, uses or condones violence, including acts of terrorism, to reach a specific political or ideological purpose[115].

The mass radicalisation of individuals in the modern era is not unprecedented: the twentieth century featured the radicalisation of some societies (e.g., Nazi Germany), and of individuals who supported the multi-national movements (e.g., Comintern) in the inter-war years. During the 1970s, individuals in western Europe were drawn to nationalist and ideologically-motivated terrorist movements. In the last forty years, individuals across the Middle East and North Africa were slowly drawn to various resistance and jihadi movements, with individuals from western Europe increasingly joining those jihadi movements' descendants in the last twenty years.

Acknowledging that radicalisation is not a new phenomenon, the European Commission notes that the trends, means, and patterns of radicalisation evolve, and responses have to be continuously adapted:

> ... home-grown lone actors and (returning) foreign terrorist fighters raise security issues and specific challenges for prevention work. Internet platforms, including social media, can be abused by violent extremists, terrorist groups and their sympathisers by providing new opportunities for mobilisation, recruitment and communication[116].

There are two dimensions to radicalisation processes: **grievances** that directly drive radicalisation of individuals and groups; and **narratives** that actively seek to solicit support, recruits, and to otherwise incentivise membership. This chapter overviews prevention measures that can **disrupt** radicalisation across both dimensions.

[114] House of Commons Home Affairs Committee, 'Radicalisation: the counter-narrative and identifying the tipping point', Eighth Report of Session 2016–17, HC 135, p. 9, available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/135/135.pdf

[115] European Commission, Migration and Home Affairs, 'Prevention of Radicalisation', available at: https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/radicalisation_en

[116] European Commission, 'Prevention of Radicalisation'.

Prevention in a Counter Terrorism and P/CVE Context

Credible practices that disrupt terrorists' operational objectives of **disorientation, target response,** and **gaining legitimacy** are vital to disrupt the **pull and push factors** that drive radicalisation. In line with the Council of Europe's overall strategic counter-terrorism P/CVE approach of **prevention**, **prosecution**, and **protection**[117], this chapter focuses on multi-faceted issues of **prevention,** particularly in the context of education, countering disinformation, and monitoring, placed in the broader context of:

> **Preventing terrorism:** through criminal law and law enforcement measures aimed at disrupting attacks or their preparation and through multifaceted longer-term measures aimed at preventing radicalisation, including countering recruitment, training, the dissemination of terrorist ideology and the financing of terrorism[118]

Beyond orientation, the triple challenge of training, coordination, and implementation is one that faces government institutions and all their C/PVE focal points and stakeholders. The European Union places this challenge at the centre of its four-pillared prevention strategy, stating in its Counter-Terrorism Agenda that the approach:

> ... sets out ways of supporting local actors and building more resilient communities as a matter of priority, in close coordination with Member States, taking into account that some attacks have also been carried out by Europeans, raised within our societies, who were radicalised without ever having visited a conflict zone[119].

This prevention Agenda has five components with related action points for the Commission, the European Parliament, European Council, and EU Member States:

- Countering extremist ideologies online
- Supporting local actors for more resilient communities
- Prisons, rehabilitation, and reintegration
- Foreign terrorist fighters and their family members,
- Consolidating knowledge and support[120]

Crime prevention in a C/PVE planning context

In thinking about how to disrupt radicalisation, the process of radicalisation prevention has some similarities to crime prevention, particularly in terms of whole-of-government and whole-of-society cooperation. Although extremists seek to go beyond a criminal act to use systematic violence for a supposed political end, the EU's Radicalisation Awareness Network notes that preventing violent extremism is crime prevention in a broad sense, and the general principles and mechanisms of crime prevention are generally applicable to C/PVE.

[117] Council of Europe, 'Objectives', Council of Europe Counter-Terrorism Strategy (2018-2022), CM (2018), 4th July 2018, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808afc96

[118] Council of Europe, 'Objectives, Council of Europe Counter Terrorism Strategy (2018-2022). Also see the section on 'European Definitions – Prevention Objectives' in Chapter Three of this book.

[119] 'Introduction', Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond', COM(2020) 795 Final, Brussels, 9th December 2020, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:795:FIN

[120] '2. PREVENT', European Commission, 'A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond'.

The comprehensive structure of crime prevention programming provides a framework for strategising counter-radicalisation programming. Crime prevention programming is conducted at four levels across different target groups:

- **Primary prevention** is targeted at whole population groups or everyone within a broad category;
- **Secondary prevention** is targeted at defined risk groups prone to committing criminal acts;
- **Tertiary prevention** is targeted at problem groups and individuals who demonstrate problematic behaviour;
- **Individual prevention** is targeted at (potential) victims of crime in order to reduce harm to individuals and to society as a whole[121].

Combining three approaches to prevention (criminal justice- based prevention, social crime prevention, and situational crime prevention), nine generic preventative measures can be applied to all forms of crime, including violent extremism:

1. Establishing and maintaining normative barriers
2. Reducing recruitment
3. Deterrence
4. Disruption
5. Incapacitation
6. Protecting vulnerable targets
7. Reducing harm
8. Reducing rewards
9. Desistance and rehabilitation[122]

This holistic model reflects the need for a broader whole-of-society approach to prevention, with law enforcement one actor in implementing mechanisms: Other actors may include civil society and community organisations, social workers, politicians, and prison and probation services, all of whom have different measures at their disposal to activate one or more of the nine prevention mechanisms[123].

vvConsequently, this comprehensive approach can be reflected in the strategic design and multi-stakeholder emphasis of national P/CVE action plans. The plans can focus on prevention at the national, regional, and local level, and specify the role of national institutions and respective stakeholders at each level. As elaborated in Chapter 3, the plans offer an opportunity for governments to identify which stakeholders hold political responsibility for activities, and to identify current and future funding sources for each activity.

Grievances, Vulnerabilities, and Prevention

To prevent radicalisation, states need to avoid bad practices that create or drive grievances across one or more segments of society. This need relates to the general conduct of security sector personnel, but also to other public service providers. Failure to address these issues through improved training and capacity development leaves states vulnerable to extremists exploiting a variety of grievances, whether real or imagined.

[121] Radicalisation Awareness Network, 'Lessons from crime prevention in preventing violent extremism by police', RAN Issue Paper, 15th January 2020, p. 2, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-pol/docs/ran_pol_lessons_from_crime_prevention_012020_en.pdf

[122] RAN, 'Lessons from crime prevention', p. 3.

[123] RAN, 'Lessons from crime prevention', p. 3.

Preventing grievance in day-to-day service provision

In order to prevent accusations of discrimination or exclusion, governments need to ensure everyday life for wider society and groups at high risk of radicalisation features equal access to services, as well as protection from security threats. This general requirement assumes that citizens can equally access a variety of socio-economic services including administrative, housing, medical, and education services. Inherent in this requirement is that citizens have equal access to security provision, principally through law enforcement services.

Preventing grievances over abuse of individual rights

Ensuring that the provision of public security does not exclude or alienate individuals or groups remains vital to prevent disaffected individuals joining radicalised groups in the first instance. Any violations of individual rights – especially repeated or systematic violations of those rights – can create a critical mass of extremist sympathisers including individuals who feel insecure due to a lack of reliable public security and lead to irrevocable breach between state and citizens. Ensuring security policy and practice is tailored to ensure good conduct and restraint is a vital means to ensure grievances are not triggered in the first instance.

Box 1. Abuse of Individual Rights – Radicalisation in Western Europe

After working in the UK Ministry of Defence, Eamon Collins returned to Ulster in 1974 to study Law at Queen's University Belfast. Returning home to his parents' home in South Armagh during a holiday, he, his teenage brother, and father were manhandled by British troops who has stopped their car at a checkpoint while looking for weapons and explosives. There were then interrogated and assaulted. At that point Collins volunteered to join the PIRA, working for the UK government as a customs agent in the daytime and for the PIRA at night[124].

Preventing Overreactions to Terrorist Threats

Similarly, any overreaction to terrorist threats themselves can create further, sometimes irrevocable, grievances and accelerate radicalisation processes within a country. Any repressive measures that broadly deny freedom of expression, freedom of assembly and freedom of association, or that criminalise protests or suppress public debate, can fuel public anger against state institutions. These grievances – and the threat of terrorism – can be exacerbated by any specific measures against individuals or groups that result in:

- detention, sometimes for protracted periods, without charge;
- denial of the right to challenge the lawfulness of detention;
- denial of access to legal representation;
- monitoring of privileged conversations with legal counsel;
- secret incommunicado detention; and ill-treatment, even torture, of detainees as well as inhumane and degrading conditions of detention;
- abduction (sometimes referred to as rendition) to another country;
- discrimination and racial profiling[125].

By avoiding and eliminating these bad practices, states have an immediate opportunity to ensure the credibility and legitimacy of their counter terrorist and C/PVE programming.

[124] 'The Price of Courage', *Newsweek*, 28th March 1999, available at: https://www.newsweek.com/price-courage-163782

[125] See OSCE ODIHR, *Countering Terrorism, Protecting Human Rights: A Manual*, 2008, pp. 20-21, available at: https://www.osce.org/odihr/29103

Box 2. Overreactions to Terrorist Threats – Internment without Trial

After imposing direct rule in Northern Ireland, the introduction of 'Internment Without Trial' (1971-1975), by the UK government was politically counter-productive. At the request of the Northern Ireland government, persons suspected of involvement in terrorism were arbitrarily detained by the state and often interrogated. During the period, a total of 1981 people were detained, often on the basis of unreliable intelligence. During one mass-internment operation alone in August 1971, 342 people were arrested in one day: the operation led to four days of violence during which 7000 people fled their homes, and twenty civilians, two PIRA members, and two British soldiers were killed, with twenty-three of them dying between 9th-10th August in the so-called 'Ballymurphy Massacre'[126].

Education

Both the educational process and the education sector itself are vital to prevent the spread of extremist narratives and behaviour. The general educational process – creating educated citizens who can independently evaluate information they read on social or other media, access and interact with government, institutions, and agencies – is crucial to limit radicalisation in general. Well-educated citizens can usually discern the reliability of sources of information and interact with government representatives and institutions.

In the context of contemporary online radicalisation, teachers can teach specific skills to their pupils. Education can be considered a component of teaching **democratic** and **civic values** in general, and of building **digital literacy** and '**cyber citizenship**' skills in particular[127]. In this context, educators and P/CVE professionals can teach **media literacy** and **online safety** in order to recognise propaganda, radicalisation narratives, fake news and conspiracy theories, a process that can also include the private sector, media, local and religious communities, and civil society[128].

Secondly, just as they monitor for signs of other negative behaviour, educators are well-placed to monitor for signals of radicalisation and identify at-risk individuals. The Council of Europe's Counter-Terrorism Strategy identifies a crucial role for 'Awareness-raising on radicalisation and other preventive measures among frontline practitioners, in particular in schools[129]', including sharing practical knowledge of how to prevent radicalisation leading to terrorism, and to identify signals or indicators of radicalisation. This guidance also applies to professionals in schools and also in youth-, sports- and community centres and in health care who should have sufficient knowledge and effective tools to actively work with preventive measures within their area of responsibilities[130].

Box 3. Switzerland's P/CVE National Action Plan: The Framework for Prevention in Education and Youth Clubs

A practical example of programming on education and youth issues is found in the Swiss P/CVE National Action Plan in which the government defines specific measures for stakeholders to implement. The Plan foresees 'Raising awareness among and providing training for key people in schools and youth clubs' (Measure 5)[131], and 'Devising

[126] See, for example, Gerry Moriarty, 'Internment explained: when was it introduced and why?, *The Irish Times*, 9th August 2019, available at: https://www.irishtimes.com/news/politics/internment-explained-when-was-it-introduced-and-why-1.3981598

[127] Peter Singer, 'Three Steps to Fight Online Disinformation and Extremism', *Defense One*, 24th January 2021, available at: https://www.defenseone.com/ideas/2021/01/three-steps-fight-online-disinformation-and-extremism/171563/

[128] Council of Europe, 'Section 1.4. Awareness Raising on radicalisation and other preventive measures among frontline practitioners , in particular in schools', Council of Europe Counter-Terrorism Strategy (2018-2022).

[129] Council of Europe, 'Section 1.4', Council of Europe Counter-Terrorism Strategy (2018-2022).

[130] Council of Europe, 'Section 1.4', Council of Europe Counter-Terrorism Strategy (2018-2022).

[131] Swiss Security Network (Sicherheitsverbund Schweiz), *Swiss National Action Plan to Prevent and Counter Radicalisation and Violent Extremism*, 4th December 2017, p. 15, available at: https://www.newsd.admin.ch/newsd/message/attachments/50703.pdf

and providing pedagogical materials for use in and outside schools' (Measure 9), including the development of a school-specific manual to 'Promote Integration, Recognise Radicalisation', as well as online resources for preventing terrorism and violent extremism[132]. Underpinning this overall approach is a dedicated multi-stakeholder approach to 'Enhancing measures to encourage active citizenship, strengthen democracy and prevent discrimination' (Measure 18)[133].

Countering Disinformation

The challenge of countering disinformation in the age of social media is significant, and complicated by the reprise of state-level 'active measures' to promote disinformation across media platforms[134]. However, beyond ensuring citizens are sufficiently educated to discern false or misleading information, whether in terms of 'digital literacy' or 'cyber citizenship', a five-step approach can limit the impact of disinformation and disrupt its effectiveness.

Countering disinformation across society comprises five steps to ensure: the availability of reliable information; that government policy objectives are clear; that institutions' practices are uncontroversial; that disinformation narratives are actively countered; and that government reacts to crises with reliable information.

The principal element of countering disinformation is to ensure that the national media sector is independent and shares reliable information. A well-capacitated media, reflecting balance and depth in its reporting, enhances public trust and confidence in news sources. Independent media regulators are one means of achieving this goal, with broadcasting licenses contingent on supplying balanced reporting.

Secondly, government needs to ensure that counter terrorism policies are clearly understood by the general public, and that institutions follow the policies. This approach limits any ambiguity over the objectives of state policy that extremists can exploit. The same principle feeds into the third step of ensuring that government's security providers abide by best practice when implementing policy: any missteps or controversial actions can feed grievances that extremists can exploit within society.

Fourthly, disinformation and propaganda need to be actively countered. Institutions need to proactively identify and flag disinformation. By monitoring sources of disinformation or radicalisation narratives, particularly on social media channels, governments have an early opportunity to flag disinformation and formulate a public response that disrupts the propaganda channels' effectiveness. Government and other stakeholders need to construct narratives that emphasise the costs, illegitimacy, and lack of credibility of extremist narratives. In parallel, governments need to avoid allegations of arbitrary censorship. Striking an appropriate balance can be difficult in extreme circumstances, but this challenge is essentially the same as in any other crisis management situation. Some remedies exist, such as time limited censorship that may be necessary in extraordinary circumstances.

Box 4. Switzerland's P/CVE National Action Plan: Counter Narratives and Alternative Narratives

The Swiss P/CVE National Action Plan has a measure dedicated to counter narratives and alternative narratives.

[132] *Swiss National Action Plan*, p. 16.

[133] *Swiss National Action Plan*, p. 19.

[134] For examples of Russian disinformation, see, for example: Reuters Staff, 'German Government Accuses Russian media of biased reporting', *Reuters*, 19th February 2016, available at: https://www.reuters.com/article/germany-russia-media-idINL8N15Y3H3 **;** Stefan Meister, 'The "Lisa case": Germany as a target of Russian disinformation', *NATO Review*, 25th July 2016, available at: https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html ; Mark Galeotti, 'Controlling Chaos: How Russia Manages its Political War in Europe', *ECFR Policy Brief*, 1st September 2017, available at: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/ ; Jeffrey Mankoff, 'Russian Influence Operations and Germany and Their Effect', *CSIS Commentary*, 3rd February 2020, available at: https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect

Measure 20 addresses 'Prevention of radicalisation, in particular via the Internet, by means of counter narratives and alternative narratives' with the rationale that people who look for or come across violent extremist propaganda on the internet must be able to find other perspectives and counter arguments in order to keep a critical distance and to build a positive identity. The development and dissemination of counter narratives and/or alternative narratives on the internet and offline is supported by initiatives in civil society and includes as many people in the target group as possible[135].

Finally, as with any response to terrorist activity in general, in crises it is crucial that government cite reliable sources and reliable media. Failure to share reliable information can damage credibility and trust and undermine other strategic responses to extremist activities. At the same time, in countering propaganda, governments need to be careful to avoid accusations that they are creating propaganda themselves[136].

Governments also need to be proactive in their communication, particularly strategic communications, on P/CVE issues. By proactively identifying the nature of terrorist threats, outlining the types of risks, and elaborating the national strategic response to terrorism, confidence can be created in the national approach to the problem. Ambiguity or lack of communication creates an information vacuum in which public trust is quickly degraded.

Monitoring

State and society need to monitor a variety of social groups and media to detect radicalisation processes. At the community level of 'everyday' monitoring, law enforcement, educators, and community groups need to watch for signs of radicalisation, extremist propaganda, or any other radicalisation activities. This approach ensures accessibility and visibility on the part of service providers who need to be seen by and accessible to local communities. In parallel, ensuring accessibility counters any sense of 'alienation' across broader society, or of an area falling beyond the control of government institutions. The overall effectiveness of monitoring depends on how active citizens and institutions are in detecting signs of radicalisation and sharing them with the wider community, government representatives, and P/CVE focal points.

Monitoring in Youth and Education

Many countries have introduced monitoring programmes in the education sphere, but tailoring these effectively is important, and is similar to monitoring other types of potentially anti-social or criminal behaviour. For example, as per the Swiss National Action Plan, training is available to orient stakeholders beyond government to detect signs of radicalisation.

Box 5. Switzerland's P/CVE National Action Plan: Training for P/CVE Monitoring

A top priority of the Swiss National Action Plan, Measure 2 focuses on 'Offers of basic and continuing education and training for experts'. The measure foresees that, in basic and continuing education and training courses, experts discuss the issue of radicalisation and violent extremism, and are made aware of how to recognise the signs and risks of radicalisation at an early stage and to act accordingly in order to prevent increased radicalisation. Experts also learn how to deal with people who may have been radicalised. The target group for this training is expansive and focused on multiple stakeholders: youth and (school) social workers, teaching staff, apprenticeship supervisors in host companies, prison staff, police, intelligence services, adult and juvenile prosecution services, juvenile court judges, asylum and migration authorities, residents' services, child and adult protection authorities, courts, professional guardians, professional personnel in the armed forces and civil protection services[137].

[135] *Swiss National Action Plan*, p. 20.

[136] For an example of a controversial approach to countering jihadi propaganda, see: Piers Robinson, 'The British government has already forgotten the great dangers of propaganda', *The Guardian,* 3rd May 2016, available at: https://www.theguardian.com/commentisfree/2016/may/03/british-government-propaganda-counter-terrorism-muslim-communities

[137] *Swiss National Action Plan*, pp. 13-14.

Online Monitoring – Passive Approaches

New forms of passive and non-intrusive online monitoring are available to government stakeholders. As social media channels are instrumentalised for terrorist recruitment, opportunities exist to automatically detect 'hate speech' used in radicalisation processes, with some methods already having over 80% accuracy[138]. The Global Internet Forum to Counter Terrorism's 'Working Group on Content-Sharing Algorithms, Processes, and Positive Interventions' shares algorithms and processes to identify risk mitigation and opportunities for positive interventions, while countering the consumption of specific content that could increase user interest[139].

One more recent development from which counter-terrorist and P/CVE professionals can benefit is the proliferation of open-source investigation organisations and specialists who monitor a variety of social media channels for information on new developments in conflict zones. Although these include some focused on state activity[140], some individuals comprehensively monitor radicalisation and extremist networks in real time[141].

Online Monitoring – Surveillance and Interception of Communications and Bulk Data

In terms of more intrusive monitoring related to suspicions of individuals' involvement in terrorism, any surveillance component needs to be in line with international and European best practice outlined in Chapter Two's 'Policy and Legal Challenges' section.

The need for any interception of communications to be evidence based, proportionate, and time-limited remains constant. Ensuring the legitimacy of any intercept is vital for any counter-terrorist prosecutions. At the same time, there is a need for technical and human surveillance capacities, some of which can be provided by existing investigations branches of law enforcement, but additional capacity may be required for dedicated counter-terrorist investigations. As a broad guide, the initiative 'about:intel' at the non-profit Stiftung Neue Verantwortung collates contemporary guidance on surveillance law, bulk collection of data, and interception of communications[142].

Online Monitoring – Combining Approaches

Due to the current proliferation of influence operations in the United States, the importance of building a multi-stakeholder community to monitor many types of influence operations is now seen as a crucial first step towards countering misinformation and propaganda that drives a variety of anti-democratic extremist activities. Countering influence operations requires not just data from companies and collaboration among researchers[143], but also inputs from policymakers themselves[144]. This approach foresees the creation of a multi-stakeholder research and development centre (MRDC) as independent venue where tech industry and external researchers can come together for a sustained period to collaborate on

[138] Tom De Smedt, Guy de Pauw, and Pieter Van Ostaeyen, 'Automatic Detection of Online Jihadist Hate Speech', *Computational Linguistics & Psycholinguistics CliPS Technical Report Series*, CTRS 007, February 2018, available at: https://www.academia.edu/36127816/Automatic_Detection_of_Online_Jihadist_Hate_Speech

[139] https://gifct.org/working-groups/

[140] See, for example, https://www.bellingcat.com and https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/.

[141] See, for example, https://twitter.com/p_vanostaeyen, https://twitter.com/ajaltamimi , and https://www.twitter.com/lindseysnell

[142] See: https://aboutintel.eu/

[143] Kelly Born, 'Building a community to counter influence operations: Four questions for Alicia Wanless ', *Hewlett Foundation*, 29th March 2021, available at: https://hewlett.org/building-a-community-to-counter-influence-operations-four-questions-for-alicia-wanless/

[144] See, for example, Carnegie Endowment for International Peace, 'Partnership for Countering Influence Operations', available at: https://carnegieendowment.org/specialprojects/counteringinfluenceoperations

monitoring and programming issues within a common structure: ‘it’s more than a vehicle for data sharing, but a bridge organization that can vet researchers, address contracting issues, and sustain longer-term research projects’[145].

Intervention

Each of the thematic prevention areas outlined in this chapter requires a capacity for government, institutions, and stakeholders to decisively intervene and disrupt radicalisation processes. Some of these interventions will occur below the threshold of criminal activity required prosecution, but it is important to note that the expansive definitions of terrorist activity outlined in the ‘Legal Dimensions’ section of Chapter Three also allow interventions by law enforcement and criminal justice sectors to prevent the commissioning of terrorist acts.

In addressing specific intervention to prevent radicalisation, intervention can be targeted at a variety of levels once evidence of radicalised behaviour is identified. The objective of each intervention is to disrupt extremist activity in whatever form it is identified.

In the online arena, whether social media or on websites, identifying and flagging sources of disinformation and propaganda remain vital to create counter narratives, disrupt terrorist communications, and alert society to an extremist channel.

In this general context, but particularly in crises, governments need to engage with technology companies to disrupt extremist platforms. Improving the responsiveness of tech companies remains an important agenda item, but, by May 2016, several technology companies that play an unintended but significant role in the proliferation of hate speech, including Facebook, Google, Microsoft, and Twitter, jointly agreed to a European Union Code of Conduct to remove illegal online hate speech within 24 hours[146]. The Terrorist Content Analytics Platform[147] promotes tech companies’ role in tackling terrorist use of the internet, and the Global Internet Forum to Counter Terrorism provides broad guidance for stakeholders on these issues[148].

In schools and youth groups, as per the previous section on ‘Education’, young people – who are often at risk of being radicalised in a variety of contexts – need to be monitored for signs of radicalisation, with decisive action taken when signs of radicalisation are identified. These young people may not yet have crossed the criminal threshold of terrorist activity but are at risk of doing so later. Creating measures to disengage young people from extremist activity prior to crossing any threshold of criminal activity requires dedicated resources.

Box 6. Switzerland’s P/CVE National Action Plan: Intervention Measures to Target Youth & to Encourage Disengagement and Reintegration

The Swiss National Action Plan elaborates a number of intervention strategies to address radicalisation amongst youth. Measure 19 identifies a need to proactively ‘target intervention in the case of children and adolescents whose safety or development is or could be endangered’, foreseeing that youth who are exposed to crisis situations or difficult circumstances are offered voluntary counselling or support services supervised and organised by trained experts, but not ordered on a compulsory basis by child or adult protection authorities[149]. In tandem, Measure 21 ‘Measures to encourage disengagement and reintegration’ foresees a specific sub-measure on ‘Disengagement measures for children and adolescents’ with youth who are classified as radicalised and requiring specific forms of

[145] Kelly Born, ‘Building a community to counter influence operations’, 29th March 2021.

[146] Alex Hern, ‘Facebook, YouTube, Twitter and Microsoft sign EU hate speech code’, *The Guardian*, 31st May 2016, https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code

[147] See: https://www.terrorismanalytics.org/about

[148] https://gifct.org/working-groups/

[149] *Swiss National Action Plan*, p. 19.

intervention and supervision that differ from those for adults, all of which must take place as early as possible. To this end, the Plan specifies that the unit for child and youth forensics at the Swiss Society of Forensic Psychiatry (SSFP) 'is developing a catalogue with specific disengagement measures, which will be used by the services for child and youth forensics at cantonal psychiatric clinics. The measures will take an interdisciplinary approach and can be applied outside criminal proceedings on request by the responsible cantonal authority'[150].

Finally, there is a general need in wider society to monitor for signs of radicalisation amongst broader socio-economic and ethnic groups. Intervention to pre-empt radicalisation is as important as intervening after signs of radicalisation are detected. For example, monitoring for signs of discrimination against a particular group, and intervening to end the discrimination, can prevent radicalisation later. The Swiss Action Plan's Measure 18 to 'Enhance measures to encourage active citizenship, strengthen democracy and prevent discrimination' contains a sub-measure focused on targeting potential victims of discrimination. To this end the Swiss federal and regional governments support the development and expansion of advice centres for victims of discrimination in all cantons. The policy basis is to prevent the development of grievances, noting that 'Experiences of discrimination and ostracism, marginalisation, human rights, violations and collective victimisation are recognised as potential factors leading to radicalisation[151]'.

Overall, it is important to note that the frequency of the interventions may be limited or rapidly decrease after a peak in terrorist activity. For example, the UK's sometimes controversial 'Prevent' programme currently receives a limited number of referrals – even after it was expanded to include right-wing extremists – and only one in ten referrals leads to targeted intervention[152]. The challenge all societies face is to retain the capacity to act decisively once signs of radicalisation are identified.

[150] *Swiss National Action Plan*, p. 20.

[151] *Swiss National Action Plan*, p. 19.

[152] Jamie Grierson, 'Prevent figures show only one in 10 anti-radicalisation referrals need acute support', *The Guardian*, 19th December 2019, available at: https://www.theguardian.com/uk-news/2019/dec/19/prevent-figures-show-only-one-in-10-anti-radicalisation-referrals-need-acute-support

Chapter Five: Cooperation between State and Society in P/CVE

To ensure the safety of their citizens, all democratic states require a comprehensive whole-of-society approach to counter-terrorism and preventing violent extremism. The long-term effectiveness of any P/CVE strategy is improved by a whole-of-government and whole-of-society approach in which institutions not only systematically perform their specified roles but also dynamically cooperate with other societal stakeholders to disrupt terrorists' activities and prevent extremism. Additionally, any substantive cooperation between state and society offers an opportunity to integrate approaches that break the cycle of grievance driving radicalisation.

To achieve these objectives, a clear strategic framework for counter-terrorism and P/CVE needs to be developed, collective and individual institutional goals need to be specified, stakeholder capabilities need to be built and maintained, and adequate resources need to be attributed to counter-terrorism and P/CVE -specific capabilities across society. At the same time, a whole-of-society approach requires civil society, communities, and the education sector to cooperatively monitor for signs of radicalisation, and to manage the reintegration of former extremists into society. This chapter outlines practical cooperation formats to achieve these common goals.

Policy and Resource Management Challenges

As with other security challenges they face, societies need to adopt a multi-dimensional approach to counter-terrorism and P/CVE. To ensure maximum effectiveness in preventing and countering terrorism, states need to address the broad policy, strategic, and legislative frameworks for countering terrorism, specify the roles and tasks of a broad range of government ministries and agencies, and adopt a whole-of-government and whole-of-society approach to prevention. This final step comprises establishing a broad, inclusive network of stakeholders and practitioners to coordinate a range of counter-terrorism and P/CVE programmes.

Policy Dimensions

The policy framework for P/CVE seeks to prevent extremism by disrupting extremists' operational objectives of **disorientation**; **target response**; and **gaining legitimacy,** and also to disrupt the **pull and push factors** that drive broader radicalisation. In adopting a strategic approach to P/CVE and counter-terrorism, policy documents are crucial to consolidate both a **whole-of-government** and **whole-of society** approach to P/CVE issues which ensures credible and legitimate practices.

As outlined in Chapter Three, P/CVE Action Plans define a broad range of prevention activities and create a common societal understanding of multiple stakeholders' responsibilities in countering extremism[153]. The **UN Action Plan**[154] published in late 2015 remains a reference point for developing a comprehensive approach to radicalisation prevention, and four of its seven thematic areas aimed at disrupting the drivers of extremism are the focus of this chapter: **Dialogue and Conflict Prevention**, **Engaging Communities**, **Empowering Youth**, and **Education**[155].

[153] Peter Neumann, 'Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region', OSCE, CIO.GAL/189/17, (September 2017), pp. 45-46, available at: https://www.osce.org/chairmanship/346841

[154] Report of the Secretary General, 'Plan of Action to Prevent Violent Extremism', A/70/674, 24th December 2015, pp. 7-10, available at: https://www.un.org/counterterrorism/plan-of-action-to-prevent-violent-extremism and https://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674

[155] Report of the Secretary General, 'Plan of Action to Prevent Violent Extremism', pp. 14-20. For additional guidance on

Switzerland's '**National Action Plan to Prevent and Counter Radicalisation and Violent Extremism**[156]' serves as a comprehensive example of putting these thematic priorities into national practice. The Plan's four goals aim to create 'practicable pre-conditions for preventing and countering radicalisation and violent extremism in all its forms', while at the same time 'respecting fundamental and human rights'[157], through a whole-of-society approach towards achieving national prevention goals focused on: **Cooperation and effective structures**; **Coordination**; **Instruments**; and **Inclusion and Support of Civil Society**[158].

The Plan's multi-dimensional approach incorporates many institutions and a focus extending to the community and local level, with the plan being formulated at federal and cantonal level by directors of **Social Services**, directors of **Education**, the association of **communes** and the union of **cities**, as well as **Justice** and **Police** directors[159]. This inclusive – and necessarily expansive – approach is emphasised in the first 'cooperation' goal of the plan. As the strategy is 'developed at local level (canton, region, city) and supported at a political level'[160], and specifies the relevant stakeholders and the common C/PVE approach, the Plan recommends:

> ... that **school authorities**, **social services**, **social** and **youth workers**, **child and adult protection authorities**, **psychiatric services**, **police**, **intelligence services** (depending on the context at federal or cantonal level), **cantonal and juvenile prosecution services**, **integration agencies** and **other specialist agencies** be involved as well as those in the immediate environment of the person [at risk of radicalisation] concerned, depending on the situation[161].

In this format, the Plan seeks to identify problematic developments and potential risks of extremism and violence as early as possible and to initiate – in an inclusive format – suitable preventative measures across state institutions and wider society.

To achieve the four national prevention goals, the Plan outlines twenty-six measures for all stakeholders to address across five thematic activity areas: **Knowledge and Expertise** (nine measures); **Cooperation and Coordination** (eight measures); **Prevention of extremist ideologies and extremist groups** (three measures); **Disengagement and reintegration** (four measures); **International Cooperation** (two measures). The plan specifies the roles and tasks of institutions and other stakeholders, such as youth groups and charities, to implement each measure from national to local level, identifies service providers and users[162], and outlines political responsibility for each measure and funding sources for each action[163].

Furthermore, the Action Plan foresees future developments to improve coordination including the formal creation of a **National Coordination Office** (Measure 16[164]) and cantonal '**Competence and Advice**

developing National Action Plans, see Also see "Guidelines and Good Practices: Developing National P/CVE Strategies and Action Plans", *Hedayah Center*, September 2016; available at: https://www.hedayahcenter.org/resources/good-practices/guidelines-good-practices-developing-national-p-cve-strategies-action-plans/ and ICCT, '12 Principles for National Action Planning', International Center for Counter-Terrorism, 30th June 2016; available at https://icct.nl/update/12-principles-for-national-action-planning/

[156] Swiss Security Network (Sicherheitsverbund Schweiz), *Swiss National Action Plan to Prevent and Counter Radicalisation and Violent Extremism*, 4th December 2017, pp. 5-6, available at: https://www.newsd.admin.ch/newsd/message/attachments/50703.pdf

[157] *Swiss National Action Plan*, p. 10.

[158] *Swiss National Action Plan*, p. 10.

[159] *Swiss National Action Plan*, p. 5.

[160] *Swiss National Action Plan*, p. 10.

[161] *Swiss National Action Plan*, p. 10.

[162] 'Annex', *Swiss National Action Plan*, pp. 31-32.

[163] 'Masterplan', *Swiss National Action Plan*, pp. 27-29. In the case of the Norwegian Action Plan, the responsibility for each measure is attributed to a particular ministry only. See, Norwegian Ministry of Justice and Public Security, 'Action Plan against Radicalisation and Violent Extremism', p. 3.

[164] *Swiss National Action Plan*, p. 18.

Centres' focused on C/PVE issues in general and performing an **early warning** function (Measure 10[165]) in particular to facilitate comprehensive whole-of-society P/CVE programming.

Resource Management Dimensions

As discussed in Chapter Three, resource management challenges specific to whole-of-society P/CVE programming can be anticipated in the requirement to develop specific P/CVE capacities across stakeholder groups, and to ensure the effective coordination and maintenance of P/CVE activities.

This requirement usually includes P/CVE training for all stakeholders so that P/CVE objectives, methods, and best practices are uniformly understood. Another requirement is to ensure a network of focal points is in place to adequately address P/CVE issues, to develop policy, and to maintain new P/CVE-specific capacities. In parallel, there is the need for a comprehensive national P/CVE coordination capability via a whole-of-government and whole-of-society framework that pools policy-makers, societal stakeholders, service providers, and the security sector, to review policy and practice and share information on extremist activities.

Sourcing additional resources for a national P/CVE coordination network can be placed in the context of wider crime prevention, but burden sharing – and maximising the contribution of existing training and information sharing networks – offers an opportunity to optimise the management of resources. The costs of many P/CVE-relevant institutional capabilities and requirements are already incorporated into national and institutional budgets. Human and financial resources required for front-line staff and infrastructure to provide basic services across a country are already incorporated into a national budget, and many service providers deal with P/CVE issues as another component of their standard portfolio.

Any additional resources required for specific P/CVE measures across society can be identified through an assessment of terrorist and radicalisation threats facing a society, and then be exhaustively itemised in a National Action Plan. All nations face the challenge of reaching a political consensus on the total number of measures required to prevent extremism and to match adequate resources to those requirements.

Attributing additional resources to meet P/CVE challenges is a political decision: linking requirements to both existing and new budget lines is crucial to ensure the transparency and efficiency of the policy and resource management processes. In the case of Switzerland, each measure specified in the C/PVE Action Plan is attributed to a specific budget[166], or – if the plan acknowledges that additional resources may be required for a particular purpose – identifies the future legislative and budgetary context for those resources to be supplied. For example, the Swiss National Action Plan sometimes emphasises that training institutions need to supply relevant content and services out of their existing budget[167], or that particular threat management activities draw on an established budget line[168], or identify the context for a wholly new budget line to be created.

Ultimately, any additional financial requirements are dependent on the terrorist threat level and radicalisation risks – the more prevention is successful, the lower the costs of maintaining P/CVE capabilities will be.

[165] *Swiss National Action Plan*, p. 16.

[166] *Swiss National Action Plan*, pp. 27-29.

[167] For example, 'Measure 4: Training of support workers in the federal centres and the cantonal centres for asylum seekers', and 'Measure 5: Raising awareness among and providing training for key people', *Swiss National Action Plan*, p. 15.

[168] 'Measure 14: Development and introduction of the concept of threat management', *Swiss National Action Plan*, p. 17.

Dialogue, Engagement, Feedback and Partnership

As outlined in the previous section, a dynamic and constructive relationship between state and society provides the foundation for effective whole-of-society P/CVE programming. Each stakeholder has different prevention challenges to address and different roles to perform. The key challenge is to establish the framework for that cooperation so that civil society in its broadest terms – in particular, families, women, youth, educators, and religious and community leaders – are all engaged in P/CVE programming[169].

The use of **whole-of-society partnerships** to address P/CVE issues can create the space for constructive engagement between state and its citizens, foster trust and understanding, widen ownership of P/CVE policies and strategies, and provide feedback and monitoring data on the impact of P/CVE policies and strategies. These partnerships can overcome initial barriers to cooperation, including any lack of prior mechanisms for co-ordination and co-operation, and provide a basis for longer term whole-of-society cooperation[170].

A whole-of-society P/CVE coordination framework and related networks offer a structure in which multiple institutions and stakeholders can work towards common prevention goals. A formal P/CVE cooperation framework allows a nation to implement a P/CVE action plan effectively, and create the space for prevention partnerships, engagement, dialogue, feedback.

The Swiss National Action Plan is an example of all the different types of roles stakeholders can perform to achieve whole-of-society P/CVE cooperation. The Action Plan specifies the cooperative roles and tasks of all stakeholders, such as **youth groups** and **charities**, to implement each of the Action Plan's measures from national to local level, identifies service providers and users[171], and outlines political responsibility for each measure and funding sources for each action[172].

The first cooperation goal of the Action Plan is premised on dialogue, cooperation, engagement, and feedback between multiple stakeholders to counter signs of extremism in individuals. Noting that prevention strategy is already 'developed at local level (canton, region, city)'[173], the Plan specifies that 'in the immediate environment of the person [at risk of radicalisation] concerned' that, as well as government institutions, '**school authorities**, **social** and **youth workers** and **other specialist agencies** be involved[174]'.

The Plan also acknowledges the need for awareness raising, training materials, and training programmes to improve all stakeholders' engagement, dialogue, engagement, and feedback roles. Measure 2 focuses on 'Offers of basic and continuing education and training for experts' on how to recognise the signs and risks of radicalisation at an early stage, how to act in order to prevent increased radicalisation, and how to deal with people who may have been radicalised[175]. Measure 5 addresses 'Raising awareness among and providing training for key people in schools and youth clubs'[176], and Measure 9 on 'Devising and providing pedagogical materials for use in and outside schools', including the development of a school-specific manual to 'Promote Integration, Recognise Radicalisation' and other online resources[177].

[169] See, for example, OSCE, *The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Guidebook for South-Eastern Europe*, 2018, p. 8, available at: https://www.osce.org/secretariat/400241

[170] OSCE, *A Whole-of-Society Approach to Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism – A Guidebook for Central Asia*, 21st January 2020, pp. 10-11, available at: https://polis.osce.org/wholeofsociety-approach-preventing-and-countering-violent-extremism-and-radicalization-lead

[171] 'Annex', *Swiss National Action Plan*, pp. 31-32.

[172] 'Masterplan', *Swiss National Action Plan*, pp. 27-29.

[173] *Swiss National Action Plan*, p. 10.

[174] *Swiss National Action Plan*, p. 10.

[175] *Swiss National Action Plan*, pp. 13-14.

[176] *Swiss National Action Plan*, p. 15.

[177] *Swiss National Action Plan*, p. 16.

Thirdly, the Action Plan also foresees broad stakeholder involvement in 'Disengagement and reintegration' of extremists, particularly in terms of sharing expertise through a national pool of experts (Measure 24)[178].

Finally, to enhance stakeholder dialogue and engagement, the Action Plan also foresees the formal creation of a **National P/CVE Coordination Office** (Measure 16[179]) and cantonal '**Competence and Advice Centres**' focused on C/PVE issues in general and performing an **early warning** function in particular (Measure 10[180]). In this way, the Action Plan not only itemises stakeholders' roles and responsibilities but also foresees the creation of more advanced and even more highly structured whole-of-society C/PVE capabilities.

Box 1: Designing Whole of Society Partnerships *As noted in Chapter Four, the EU's Radicalisation Awareness Network notes that preventing violent extremism is crime prevention in a broad sense, and the general principles and mechanisms of crime prevention are generally applicable to C/PVE, not least as many countries build partnerships with communities to prevent crime from local to national levels. The comprehensive structure of crime prevention programming provides a framework for strategising and designing whole-of-society P/CVE programming at four levels, in terms of :*

- ***Primary prevention*** *targeted at whole population groups or broad categories;*
- ***Secondary prevention*** *targeted at defined risk groups prone to criminal activity;*
- ***Tertiary prevention*** *targeted at problem groups and problematic individuals;*
- ***Individual prevention*** *targeted at (potential) victims of crime[181].*

Using this format, nine generic preventative measures can be applied to violent extremism through whole-of-society partnerships, namely: Establishing and maintaining normative barriers; Reducing recruitment; Deterrence; Disruption; Incapacitation; Protecting vulnerable targets; Reducing harm; Reducing rewards; Desistance and rehabilitation[182].

This holistic model reflects the need for a broader whole-of-society approach to prevention, with law enforcement one actor in implementing mechanisms: Other actors include civil society and community organisations, social workers, politicians, and prison and probation services, all of whom have different measures at their disposal to activate one or more of the nine prevention mechanisms[183].

Communities & Civil Society

The long-term success of P/CVE efforts hinge on the establishment of meaningful engagement and transparent partnerships among government institutions, community leaders and civil society actors. Communities and civil society not only perform a monitoring role, but also participate in **partnerships** and **problem-solving**.

[178] *Swiss National Action Plan*, p. 21.

[179] *Swiss National Action Plan*, p. 18.

[180] *Swiss National Action Plan*, p. 16.

[181] Radicalisation Awareness Network, 'Lessons from crime prevention in preventing violent extremism by police', *RAN Issue Paper*, 15th January 2020, p. 2, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-pol/docs/ran_pol_lessons_from_crime_prevention_012020_en.pdf

[182] RAN, 'Lessons from crime prevention', p. 3.

[183] RAN, 'Lessons from crime prevention', p. 3.

Civil Society

OSCE have identified seventeen guidelines outlining the roles civil society and communities can play in P/CVE, and the ways in which government stakeholders can support their role[184]. In summary, effective civil society-led P/CVE initiatives require an environment in which:

- Civil society groups and actors can perform their work without interference and in line with the fundamental rights of freedom of expression, assembly, and association.

- Government facilitates the involvement of civil society in the full spectrum of P/CVE programming and policy development through cooperation partnerships and platforms.

- Regular engagement with CSOs is established through flexible and responsible multi-agency co-ordination mechanisms, such as: advisory committees, P/CVE information sharing centres, roundtables, and institutional alliances.

Civil society can perform important facilitation and feedback roles from national to local levels, and it is important to reflect these in national P/CVE Action Plans. Reflecting the acknowledged importance of communities and civil society, the Swiss National Action Plan establishes '**Inclusion and Support of Civil Society'** as one of four dedicated national P/CVE goals, specifying that:

> Civil society's commitment to and active participation in initiatives and projects are essential for the prevention work. Participation in the work and the decision-making process contributes to positive decisions, strengthens the feeling of social solidarity and alleviates or indeed eliminates fears, uncertainties, and discriminatory tendencies[185].

The Action Plan also identifies a crucial role for civil society in counter narratives. Measure 20 on 'Prevention of radicalisation, in particular via the Internet, by means of counter narratives and alternative narratives' (Measure 20) specifies that the:

> development and dissemination of counter narratives and/or alternative narratives on the internet and offline is supported by initiatives in civil society and includes as many people in the target group as possible[186].

As specified in the previous sections and chapters, civil society also contribute to national P/CVE coordination frameworks, dialogue, monitoring, and reintegration frameworks.

Communities

Community leaders can play a vital role as mediators between communities and government bodies. Any resulting partnerships can be useful in addressing a range of public safety concerns that include P/CVE issues. Working with credible community leaders to create a sense of common purpose on P/CVE matters is a worthwhile investment which is linked to increasing the chance of successful programming outcomes[187].

[184] OSCE, *The Role of Civil Society in Preventing and Countering Violent Extremism*, pp. 50 – 60, available at: https://www.osce.org/secretariat/400241

[185] *Swiss National Action Plan*, p. 9.

[186] *Swiss National Action Plan*, p. 20.

[187] Global Counterterrorism Forum, 'Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism', 2013, available at: https://www.thegctf.org/About-us/GCTF-framework-documents

Community leadership is not limited and it is prudent for institutions to identify and engage with a wide range of community members in terms of age, gender, ethnicity, and beliefs. It is possible to engage communities' religious leaders in P/CVE in wider roles and harness their influence on governance, human development, and peacebuilding initiatives[188].

Community leaders can have a positive impact on a range of P/CVE interventions from early-stage prevention to the rehabilitation and reintegration of extremists. In particular, community leaders have a crucial role to play in detecting early signs of extremism amongst their wider community, and this issue is addressed in detail in the 'Monitoring' section of Chapter Seven. In parallel, as credible actors with unique knowledge of what messages resonate with vulnerable members of the community, they can be highly effective communicators of alternative counter-radicalisation narratives[189].

On a day-to-day basis, in terms of community policing, community partnerships with local police law enforcement are common in many societies and serve a problem solving with communities[190]. At the same time, civil society and communities should not be instrumentalised by government agencies to provide services such as intelligence gathering as these partnerships work better in a P/CVE context when they are co-operative instead of extractive or perceived as externally directed[191].

Overall, incorporating community associations and leaders into programming with civil society enhances an inclusive national P/CVE coordination framework. Similarly, many youth groups can be considered part of community engagement on P/CVE issues, and their role, along with educators, are the focus of the next section.

Education & Engaging Youth

In both schools and youth groups, young people – who are at risk of being radicalised in a variety of contexts – need to be monitored for signs of radicalisation, with decisive action taken when signs of radicalisation are identified. The young people concerned may not yet have crossed the criminal threshold of terrorist activity but are at risk of doing so later. Creating measures to disengage young people from extremist activity prior to crossing any threshold of criminal activity requires dedicated resources for both educators and youth groups.

In this context, intervention to pre-empt radicalisation is as important as intervening after signs of radicalisation are detected. As an established best practice, in this context the Council of Europe's Counter-Terrorism Strategy identifies a crucial role for 'Awareness-raising on radicalisation and other preventive measures among frontline practitioners, in particular in schools'[192], including sharing practical knowledge of how to prevent radicalisation leading to terrorism, and to identify signals or indicators of radicalisation. This guidance also applies to professionals in schools and also in youth-, sports- and community centres and in health care who should have sufficient knowledge and effective tools to actively implement preventive measures within their responsibility area[193]. Youth leaders' crucial role to play in detecting early signs of extremism is also addressed in more detail in the 'Monitoring' section of Chapter Seven.

[188] Global Counterterrorism Forum, 'Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism'.

[189] Barzegar et. al., 'Civic Approaches to Confronting Violent Extremism: Sector recommendations and best practices', 2016, cited in: OSCE, *The Role of Civil Society in Preventing and Countering Violent Extremism*, p. 31.

[190] Peter Neumann, 'Countering Violent Extremism and Radicalisation that Lead to Terrorism', p. 52.

[191] OSCE, *The Role of Civil Society in Preventing and Countering Violent Extremism*, p. 30.

[192] Council of Europe, 'Section 1.4', Council of Europe Counter-Terrorism Strategy (2018-2022).

[193] Council of Europe, 'Section 1.4', Council of Europe Counter-Terrorism Strategy (2018-2022).

Education & the Education Sector

Both the educational process and the education sector itself are vital to prevent the spread of extremist narratives and behaviour. The general educational process – creating educated citizens who can independently evaluate information they read on social or other media, access and interact with government, institutions, and agencies – is crucial to limit radicalisation in general. Well-educated citizens can quickly ascertain the reliability of information on the internet and interact with government representatives and institutions. Additionally, a well-educated citizenry facilitates cooperative P/CVE programming as stakeholders are already educated on shared national values and can establish a consensus on any threats to those values.

In the context of contemporary online radicalisation, teachers can teach specific skills to their pupils. Education can be considered a component of teaching democratic and civic values in general, and of building digital literacy and 'cyber citizenship' skills in particular[194]. In this context, educators and P/CVE professionals can teach media literacy and online safety in order to recognise propaganda, radicalisation narratives, fake news and conspiracy theories, a process that can also include the private sector, media, local and religious communities, and civil society[195].

Secondly, as discussed in Chapter Four, educators are well-placed to monitor for signals of radicalisation and identify at-risk individuals. Just as they monitor for evidence of other negative behaviours, teachers will often be the first to detect signs of radicalisation. Educators can then alert national P/CVE coordination frameworks to radicalisation processes and radicalised individuals and initiate intervention to prevent further extremist indoctrination or other activities.

Schools and Youth Groups in Prevention Programming

The Swiss National Action Plan offers practical examples of how to create a framework incorporating the education sector and youth groups in cooperative national P/CVE policy implementation. The Plan outlines a framework for prevention in education and youth clubs in which the government defines specific measures for stakeholders to implement. The Plan foresees 'Raising awareness among and providing training for key people in schools and youth clubs' (Measure 5)[196], and 'Devising and providing pedagogical materials for use in and outside schools' (Measure 9), including the development of a school-specific manual to 'Promote Integration, Recognise Radicalisation', as well as online resources for preventing terrorism and violent extremism[197]. Underpinning this overall approach is a dedicated multi-stakeholder approach to 'Enhancing measures to encourage active citizenship, strengthen democracy and prevent discrimination' (Measure 18)[198].

National training programmes to orient stakeholders beyond government to detect signs of radicalisation also includes educators and youth workers. As a top priority of the Action Plan, Measure 2 focuses on 'Offers of basic and continuing education and training for experts'. The measure foresees that, in basic and continuing education and training courses, experts discuss the issue of radicalisation and violent extremism, and are made aware of how to recognise the signs and risks of radicalisation at an early stage and to act accordingly in order to prevent increased radicalisation. Experts also learn how to deal with people who may have been radicalised. The target group for this training is expansive and focused on multiple stakeholders including youth and (school) social workers, teaching staff, apprenticeship supervisors in host companies, as well as staff from many government institutions[199].

[194] Peter Singer, 'Three Steps to Fight Online Disinformation and Extremism', *Defense One*, 24th January 2021, available at: https://www.defenseone.com/ideas/2021/01/three-steps-fight-online-disinformation-and-extremism/171563/

[195] Council of Europe, 'Section 1.4. Awareness Raising on radicalisation and other preventive measures among frontline practitioners , in particular in schools', Council of Europe Counter-Terrorism Strategy (2018-2022).

[196] *Swiss National Action Plan* p. 15, available at:
https://www.newsd.admin.ch/newsd/message/attachments/50703.pdf

[197] *Swiss National Action Plan*, p. 16.

[198] *Swiss National Action Plan*, p. 19.

[199] *Swiss National Action Plan*, pp. 13-14.

Chapter Six: Returnees

Introduction

European nations face a significant challenge when reintegrating nationals who have travelled abroad to participate in conflicts and terrorist acts. The volume of citizens returning from Syria and Iraq is higher than those who travelled – usually unprosecuted – to Afghanistan, Chechnya, Pakistan, and Yemen between 1991 and 2001, and both the legislative and criminal justice framework have expanded to manage the increased volume. Often aggregated under the broad term 'foreign terrorist fighters' (FTFs), a variety of European citizens travelled to fight for, or to support, the Islamic State, including women, children and teenagers. There are also now cases in which children born in the conflict zone have European citizenship rights and need to be integrated into society once repatriated.

Following the Islamic State's loss of territory in Iraq and Syria, individuals have voluntarily attempted to go home, some have been repatriated by a third party, and others have been identified in refugee camps by governments and humanitarian organisations in the region. Managing the return of these diverse individuals poses a significant challenge for any society.

Dealing effectively with returnees is an opportunity to consolidate each element of an effective strategic approach to counter-terrorism in terms of **prevention**, **prosecution**, and **protection**. Furthermore, credible, and legitimate practices in regard to returnees offer an opportunity to further disrupt terrorists' ongoing operational objectives of **disorientation**; **target response**; and **gaining legitimacy,** as well as the **pull and push factors** that drive broader radicalisation. The chapter outlines current best practice related to returning FTFs and their families.

Policy, Legal, and Resource Management Challenges

Foreign fighter returnees are not a homogeneous group: the different types of FTFs returning to European societies pose a variety of challenges for policymakers and government institutions. In general, there are four types of returnees, but a fifth can also be included to improve the policy response and to manage limited resources.

Firstly, there is a major risk that some individual – and still motivated – foreign fighter returnees will attempt to conduct terrorist attacks after returning home. A second group of individuals can more be seen as victims of IS recruitment efforts. A third set of returnees fall somewhere between victims and (potential) terrorists. A fourth group are those who no longer see the use of violence as justified or necessary, either through disillusionment or the physical or psychological trauma caused by involvement in warfare or life under IS[200]. Children and youth can be added to this list: even though some fall under the second and third category, for a variety of social, legal, and policy reasons it is important to treat children taken abroad – or born abroad – as a separate group. This allows a series of dedicated measures to be applied to resocialise and reintegrate children into democratic society.

Those individuals who feel that they are again a part of society are less likely to fall back and become attracted to terrorist or violent extremist groups. To achieve this, any resocialisation process must be tailored to an individual's situation, and when supporting a returnee in his or her resocialisation process it is necessary to take stock of the reasons behind their return, their personal social situation, their mental state and their ideological convictions[201]. The following sections address this process in terms of policy, legal, and resource challenges.

[200] Bart Schuurman and Liesbeth van der Heid, 'Foreign fighter returnees & the reintegration challenge', *Radicalisation Awareness Network, RAN Issue Paper*, November 2016, p. 3, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_foreign_fighter_returnees_reintegration_challenge_112016_en.pdf

[201] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', *RAN Manual*, July 2017, p. 53, available at: https://ec.europa.eu/home-affairs/sites/default/files/ran_br_a4_m10_en.pdf

Policy Challenges

Policy needs to be designed to accommodate all types of returnees. The **reintegration** of (former) terrorists or extremists can be seen as a process aimed at facilitating their reintegration into society in a way that reduces the likelihood that they will resort to terrorism-related activity[202]. This process includes different elements. **Deradicalisation** and **disengagement** processes need to be implemented with high-risk FTFs to ensure their **rehabilitation** and renunciation of violence. At the same time, these processes need to avoid reigniting grievances that drive radicalisation in the first instance[203].

In broader terms, the fundamental policy challenge is the **resocialisation** of all returnees. This can include returning men and women: who will not be prosecuted or who have not (yet) been prosecuted; who are prosecuted but found not guilty; and those who have already served a prison sentence and who have been released and not put on probation. The resocialisation process must be tailored to an individual's situation: it is crucial to analyse the reasons for their return, their personal social situation, their mental state, and ideological convictions[204]. As part of rehabilitation and resocialisation processes, a period of **stabilisation** is crucial for returnees to consolidate the positive outcomes of previous processes[205].

Resocialisation, rehabilitation, and reintegration include prosecution and custodial phases for those found guilty of terrorist activities. However, prosecution and imprisonment does not cover all types of returnees. Consequently, an array of measures for **non-custodial rehabilitation** and **reintegration** are available and can complement those used in a pre-trial or custodial setting[206]. Some nations have overlooked the need for broader non-custodial policy remedies alongside more FTF-focused programming, but the utility of this option can be emphasised for two reasons: to mitigate risk and to complement broader institutional approaches to extremism. For example, the Canadian 'National Strategy for Countering Radicalization to Violence' emphasises that the option can complement the work of:

> security and policing agencies in monitoring, investigating, and building a case for criminal proceedings. Disengagement programmes, such as initiatives to help individuals exit from violent extremist groups, are another way of mitigating the potential threat posed by these individuals[207]

These processes involve multiple institutions, and the following sections outline how to adopt a whole-of-government and multi-stakeholder approach to implementing policy.

Legal challenges

In principle, the prosecution of returnees whose activities have crossed the threshold of supporting terrorist activities is straightforward. The key challenge, as outlined in Chapters Two and Three, is to gather evidence of criminal activity in relation to terrorism, whether general support, logistic support, or acts of violence themselves.

[202] Schuurman and van der Heid, 'Foreign Fighter returnees & the reintegration challenge', p. 3.

[203] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters" within a Human Rights Framework*, 2018, pp. 60-62, available at: https://www.osce.org/odihr/393503

[204] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', p. 53.

[205] Radicalisation Awareness Network, 'Rehabilitation Manual – Rehabilitation of radicalised and terrorist offenders for first-line practitioners', *RAN Rehabilitation Manual*, p. 5.

[206] See, for example, OSCE, *Non-custodial Rehabilitation and Reintegration in Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Guidebook for Policymakers and Practitioners in South-Eastern Europe*, 28th January 2020, pp. 15-19, available at: https://polis.osce.org/noncustodial-rehabilitation-and-reintegration-preventing-and-countering-violent-extremism-and

[207] Public Safety Canada, *National Strategy on Countering Radicalization to Violence*, 2018, pp. 16–17, available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx

Firstly, on their arrival home, returnees need to be screened for specific criminal acts considered to be acts of terrorism, including murder, kidnapping, hijacking, infrastructure attacks, and threats to commit any such acts[208]. Secondly, returnees need to be screened for additional intentional acts of terrorism, comprising:

- the act of travel and return of 'Foreign Terrorist Fighters';
- various types of terrorist financing and illicit trafficking;
- supplying services as intermediaries to terrorist groups;
- posting online terrorist content;
- soliciting terrorist offences;
- providing training for the purposes of terrorism;
- and recruiting for the purposes of terrorism[209].

The broad range of additional intentional acts – including travel itself – means that, in the absence of evidence of abduction or coercion, many female returnees may be convicted of supporting terrorism.

However, there are other legal challenges to consider. Chapters Two and Three outlined a variety of positive human rights protections to apply in the context of counter-terrorism, and legislation criminalising FTF-related conduct, and its interpretation and application in practice, needs to be clearly defined and respect international norms[210]. Criminal responsibility must also be individual and not collective[211], and the application of criminal law should not be disproportionate or arbitrary[212]. In cases where, due to a lack of evidence, returnees have not crossed the threshold for prosecution, restraint is required when imposing 'Administrative Measures'[213]. Of these measures, travel bans and the revocation of passports are two methods of choice employed by states in respect to FTFs, and states need to avoid arbitrary or disproportionate use of these measures, not least to avoid provoking additional grievances[214].

Child returnees pose specific – and in some cases, significant – legal challenges. A nation's legal response to the challenge can also have an impact on a child's **rehabilitation** and **resocialisation**[215]. The UN Counter-Terrorism Centre of the United Nations Office of Counter-Terrorism has issued exhaustive legal guidance that situates the rights of children and youth (children under the age of 18, and who were under 18 when travelling to a conflict zone) in terms of human rights[216], comprehensive guidance that is reflected in the European space by the EU[217] and OSCE ODIHR[218].

In simple terms, the best interests of a child are a primary consideration[219] when addressing the legal status of child returnees. All children have a right to be free of discrimination. In the context of returnees, there cannot be discrimination based on parents' status as the principle of non-discrimination means

[208] EU Council Framework Decision of 13 June 2002 on combating terrorism, (2002/475/JHA), OJ L 164, 22/06/2002, Art. 1(1), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002F0475

[209] Directive (EU) 2017/541 of the European Parliament and of the Council of 15th March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Articles 8-19, available at: http://data.europa.eu/eli/dir/2017/541/oj and https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A32017L0541

[210] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters"*, pp. 35-36.

[211] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters"*, p. 36.

[212] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters"*, p. 39.

[213] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters"*, pp. 46-52.

[214] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters"*, p. 51.

[215] RAN Manual, p. 73.

[216] UNOCT UNCCT, *Children affected by foreign-fighter phenomenon: Ensuring a child rights-based approach*, UNOCT UNCCT Handbook, October 2019, available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/0918_ftf_handbook_web_reduced.pdf

[217] RAN, 'Responses to returnees: Foreign terrorist fighters and their families', *RAN Manual*, pp. 73-75.

[218] OSCE ODIHR, *Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters"*, pp. 68-70.

[219] UNOCT, *Children affected by foreign-fighter phenomenon: Ensuring a child rights-based approach*, pp. 29-32.

that States must protect children from discrimination and punishment based on the “status, activities, expressed opinions, or beliefs” of their “parents, legal guardians, or family members[220].” Secondly, there cannot be any discrimination against children manipulated by designated terrorist groups. Children have a right to equal access to services that can assist in their reintegration, and reintegration measures should avoid stigmatisation and be free from negative distinctions between children who were recruited and used by designated terrorist groups and those who were not. All children who have been involved in conflict are vulnerable and should be treated primarily as victims and survivors of human rights violations[221].

In the European context, several legal issues are important when a child returns after their – or their parents' – stay in a terrorist conflict zone. Acknowledging the variation of legal norms across the EU, the EU's guidance reflects developing legal norms at international level, and what is considered to be best practice in the Union itself. The guidance reflects typical policy and legal challenges European democracies now face in regard to child returnees.

- **Nationality of the child**: nationality and citizenship depend on legal judgements within each EU country. Difficulties most often arise when the child was born in the conflict zone and there are no documents confirming the biological connection between the child and his / her parents. However, to ensure the child's reintegration, it is important to determine their legal status, and DNA testing can provide relevant evidence[222].

- **Custody of the child**: Legal determinations are country-specific within the EU, but if the parents are still together or one of the parents is seen as able to care for the child, they will receive (shared) custody. When the parent(s) are unfit to take care of the child other relatives may want to claim custody. If no solution can be found, a care-taker will receive custody and the child is likely to be placed in an institutional care. But children will often stay with the mother as female returnees are prosecuted less frequently[223].

- **Criminal prosecution of the child**: Children's combat roles in terrorist groups (e.g., as suicide bombers, as soldiers, as executioners) are documented, so questions over whether these children are legally accountable for their actions have multiplied. Per the 2016 report by the United Nations Interregional Crime and Justice Research Institute (UNICRI) on ‘Children and counter-terrorism’, the current legal framework concerning children recruited by armed or terrorist groups supports the non-prosecution of children under 18, and instead emphasises their reintegration and rehabilitation[224].

- **Rights of the child and child protection**: As all EU Member States have ratified the UN Convention on the Rights of the Child (UNCRC), they apply the basic principle behind the convention that all states act in the best interests of the child. The convention covers compliance with child custody and guardianship laws to ensure that every child has basic rights such as the right to life, to their own name and identity, to be raised by their parents within a family or cultural grouping, and to have a relationship with both parents, even if they are separated. There is also an obligation to provide separate legal representation for a child in any judicial dispute concerning their care and to ensure that the child's viewpoint be heard in such cases[225].

Following these legal best practices imposes extra resource costs on the state in terms of developing and implementing policy, but limits both the scope for grievance amongst returnees, and the legal jeopardy of the state in higher courts, whether at regional or international levels.

[220] UNOCT, *Children affected by foreign-fighter phenomenon: Ensuring a child rights-based approach*, p. 28.

[221] UNOCT, *Children affected by foreign-fighter phenomenon: Ensuring a child rights-based approach*, p. 28.

[222] RAN, ‘Responses to returnees: Foreign terrorist fighters and their families’, *RAN Manual*, p. 73.

[223] RAN, ‘Responses to returnees: Foreign terrorist fighters and their families’, *RAN Manual*, p. 73.

[224] RAN, ‘Responses to returnees: Foreign terrorist fighters and their families’, *RAN Manual*, p. 73.

[225] RAN, ‘Responses to returnees: Foreign terrorist fighters and their families’, *RAN Manual*, p. 73.

Resource challenges

Many of the human and financial resources required to address the return of FTFs and their families are already covered by existing budget allocations for and personnel working in law enforcement, penitentiary system, social services, and the education sector. However, to ensure effective planning and programming for reintegrating returnees, additional costs, human resources, and training needs can be identified in both the short and long term.

Beyond the initial cost of extricating citizens from conflict zones, returnees need to be securely hosted while screened to identify those who can be charged with terrorist activities. Forensic costs may also be incurred, including digital forensics to secure evidence on electronic devices. Screening for identify confirmation may impose an additional cost burden. Any preliminary reintegration into society imposes an additional monitoring burden wherever returnees are hosted. At the outset, these extra costs place an additional burden on the state budget as need to be done effectively and require dedicated infrastructure and extra personnel.

Some other costs are offset by standard service provision and the national C/PVE programming structure. Some pre-budgeted measures for monitoring, deradicalisation, and disengagement within societies can be used to absorb similar costs associated with returnees. For example, the Swiss C/PVE National Action Plan anticipates a range of returnee costs that will be absorbed by existing budgets and institutions. In the cases of Measure 19 **'Targeted intervention in the case of children and adolescents whose safety or development is or could be endangered'**, and Measure 23 specifying '**Expert support for families and others close to radicalised persons**', services are provided at cantonal level through the cantons' existing budget for social service directorates[226].

Similarly, the funding for significant '**Measures to encourage disengagement and reintegration**' (Measure 21) comprising a 'List of interdisciplinary disengagement and reintegration measures' and '**Disengagement measures** for children and adolescents'[227], are attributed to cantons' pre-existing budgets, as is Measure 22 elaborating the **'Competent authority for the treatment of radicalised persons outside of criminal proceedings and the execution of sentences'**[228].

However, the Action Plan notes the requirement for extra funds to sustain a long-term commitment to effective disengagement, reintegration, and resocialisation. Measure 24 on '**Creating a national pool of experts on disengagement and reintegration**[229]' foresees that:

> ... the implementation of the various disengagement and reintegration measures at local level must be based on national and international expertise. Measures must also be based on scientific studies ... To this end, a national pool of experts should be set up to offer the implementing authorities and agencies a frame of reference, provide the required specialist knowledge and take account of gender-specific differences.

The broad scope of this operational requirement is reflected in the need for experts on psychiatry, psycho-sociology, and education as well as on terrorism, violent extremism, religion, integration, and the penal system, and the National P/CVE Coordination Office. To fulfil the requirement and sustain its capacity, the measure foresees that political and funding responsibility lie at the federal level[230] via a five-year

[226] Swiss Security Network (Sicherheitsverbund Schweiz), *Swiss National Action Plan to Prevent and Counter Radicalisation and Violent Extremism*, 4th December 2017, p. 19, available at: https://www.newsd.admin.ch/newsd/message/attachments/50703.pdf

[227] *Swiss National Action Plan*, p. 21.

[228] *Swiss National Action Plan*, p. 21.

[229] *Swiss National Action Plan*, p. 21.

[230] *Swiss National Action Plan*, p. 21.

long national incentive scheme to deploy funds for new P/CVE projects initiated by cantons, communes, cities, and civil society. The incentive scheme itself is specified in a dedicated measure (Measure 17: **National Incentive Programme**[231]).

Developing a time-limited pool of funds via an incentive scheme to deal with new challenges associated with FTF returnees offers an opportunity to complement – but avoid duplicating – existing institutional capacity. The scheme also offers an opportunity to manage a surge in operational demands related to returnees, but to address the resource challenge in a transparent format.

Reintegrating Fighters

To be effectively reintegrated back into society, returned FTFs require a mixture of short- and long-term measures to successfully ensure their reintegration into society. The responsibility for this process, which can be understood as a process of both **rehabilitation** and **reintegration** of radicalised individuals and terrorist offenders, falls to the government and its agencies. While those convicted of terrorism offences will usually have a custodial sentence to serve in prison, the rehabilitation and reintegration process begins at the point of their arrival back in their country of origin.

Rehabilitation is a comprehensive process, ideally resulting in the rehabilitated person leading a self-determined and self-sustained life in a democratic society, without adhering to extremist views or participating in extremism-inspired activities (including violence)[232]. To this end, specific **rehabilitation** processes for convicted FTFs occur both inside and outside of prison[233]. For this target group, the **rehabilitation** process involves three elements:

- **deradicalisation** (behavioural disengagement from extremism-inspired activities and violence, plus cognitive distancing leading to rejection of extremist views);

- **integration** (combination of social integration into communities and functional integration into contexts such as employment, housing, and healthcare);
- a long-term period of **stabilisation**, during which positive outcomes of previous processes are internalised, reinforced, and consolidated[234].

The *Radicalisation Awareness Network* identifies seven distinct rehabilitation phases that guide the reintegration process of all returnees towards a positive outcome[235]. Each phase places responsibilities on a variety of government institutions and personnel.

- **Phase 1: Pretrial detention and investigative custody**

  The objective is to provide psychosocial support to minimise further grievances, and, in some cases, to slow down any ongoing radicalisation processes until dedicated rehabilitation work can begin after sentencing.

- **Phase 2: Reception in prison**

  The objectives are to ensure a smooth transition to life in prison, provide psychosocial support and minimise grievances, and encourage openness to engage in the rehabilitation process.

[231] *Swiss National Action Plan*, p. 18.

[232] RAN, ‘Rehabilitation Manual – Rehabilitation of radicalised and terrorist offenders’, p. 5.

[233] Dennis Walkenhorst, Till Baaken, Maximilian Ruf, Michèle Leaman, Julia Handle and Judy Korn, ‘Rehabilitation Manual – Rehabilitation of radicalised and terrorist offenders for first-line practitioners’, *RAN Manual*, June 2020, available at: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-papers/rehabilitation-manual_en

[234] RAN, ‘Rehabilitation Manual – Rehabilitation of radicalised and terrorist offenders’, p. 5.

[235] RAN, ‘Rehabilitation Manual – Rehabilitation of radicalised and terrorist offenders’, pp. 6-7.

- **Phase 3. Putting time to constructive use in prison**

  During this long phase, all relevant actors must jointly make significant strides that serve as groundwork for rehabilitation while a prisoner is serving their sentence. The objective is to motivate offenders to keep participating in all aspects of the rehabilitation process, supported by a joint effort from all relevant actors.

- **Phase 4. Preparation for release from prison**
  This crucial transition phase involves close accompaniment by relevant actors. The objective is to design a post-release plan detailing the necessary steps for offenders, once released. This plan is based on a rigorous and realistic assessment of their personal capacities and prospects of social and functional integration, after release.

- **Phase 5. The first months after release from prison**
  During this phase, ex-prisoners are likely to experience multiple crises linked to the readjustment process to life outside prison. The primary objective is to support ex-prisoners post-release throughout the readjustment, including expectation management and comprehensive accompaniment through post-prison challenges.

- **Phase 6. Reintegration into society**

  The objective is to utilise existing connections with positive social contacts, or enable the creation of new ones, as well as to expand and strengthen social and functional support networks for further long-term rehabilitation.

- **Phase 7. Stabilisation in society**

  Covering the years after individuals have been released from prison, this is the final step in rehabilitation. The objective of is to strengthen positive capacities and integration, and to achieve independence from rehabilitation support structures.

In terms of practical application of these measures, Switzerland's C/PVE National Action Plan offers detailed guidance on how government and stakeholders can facilitate the rehabilitation process. Activity Area 4.4 on '**Disengagement and reintegration**' outlines '**Measures to encourage disengagement and reintegration'** (Measure 21)[236], with the first part of the measure specifying a '**List of interdisciplinary disengagement and reintegration measures**' (Measure 21 a)) addressing the need to manage individual cases of '...any person classified as radicalised, irrespective of whether they face criminal proceedings or are serving a sentence[237]'.

To re-emphasise the importance of a comprehensive approach to disengagement and reintegration, the Plan asserts that:

> these measures should be ordered when radicalised persons face criminal proceedings and while they are serving sentences (including probation), and also outside these situations; they must also take account of the differences between the sexes[238].

The measures are governed by strict security protocols. Institutions have to factor into any reintegration programming two separate measures on '**Threat management**' (Measure 14)[239], involving cooperation with law enforcement and intelligence services, and '**Exchange of personal information and profiles between authorities**' (Measure 15a), comprising preventive policing measures specified in police count-

[236] *Swiss National Action Plan*, p. 20.

[237] *Swiss National Action Plan*, p. 20.

[238] *Swiss National Action Plan*, p. 20.

[239] *Swiss National Action Plan*, p. 17.

er-terrorism legislation, such as restrictions on travel documents (passports) and obligations to report to a police station[240].

The measure emphasises the whole-of-government nature of disengagement and reintegration processes by specifying expansive responsibilities and cooperation procedures, covering: prosecution and prison authorities; forensic psychiatric clinics; child and youth forensic services; child and adult protection authorities; professional guardians, specialist agencies, cantonal police, federal police, and the training centre for prison staff[241].

The second disengagement and reintegration measure in the Action Plan outlines the voluntary nature of reintegration outside the prison system and criminal justice process and specifies the need for regional governments to create an authority with responsibility for radicalised individuals. In defining the '**Competent authority for the treatment of radicalised persons outside of criminal proceedings and the execution of sentences'** (Measure 22) the plan specifies that each regional canton **'**should designate an authority which can offer voluntary reintegration measures' to perform the functions specified in the preceding Measure 21 a)'. While the same authority has responsibility for managing FTFs' transition from the criminal justice system, the core target group comprises 'Radicalised persons on whom the prosecution or sentence execution authorities are unable to impose measures'[242]. Beyond creating a dedicated responsible authority in each region, the measure assigns political responsibility to social services, welfare organisations, city security directors, welfare organisations, and cantonal justice and police directors[243].

In parallel, as returnees do not exist in a vacuum, the Action Plan specifies a measure to provide '**Expert support for families of and others close to radicalised persons**' (Measure 23)[244]. The measure specifies that guidelines need to be developed to support experts dealing with specific case, and measures should be devised for supporting and counselling the families and relatives of radicalised persons[245].

Reintegrating Women and Children

The seven distinct rehabilitation phases that guide the reintegration process outlined in the previous section[246] are equally applicable to female returnees. However, additional measures can be adopted to process women and children who may not have directly participated in terrorist acts. As women may have supported terrorist activity, the measures applied to them can be different to those applied to children and youth. In terms of children, as outlined in the legal challenges section, reintegration includes policy considerations that go beyond those applicable to adults. Each phase places additional responsibilities on government institutions and personnel.

Once returned, women and children require family and prevention support, including telephone hotlines[247], mental health support and screening[248], and practical measures to facilitate reintegration including registration in identification databases, immediate medical treatment, access to housing, financial and legal support, and employment and education opportunities[249].

[240] *Swiss National Action Plan*, p. 17.
[241] *Swiss National Action Plan*, p. 20.
[242] *Swiss National Action Plan*, p. 21.
[243] *Swiss National Action Plan*, p. 21.
[244] *Swiss National Action Plan*, p. 21.
[245] *Swiss National Action Plan*, p. 21.
[246] RAN, 'Rehabilitation Manual – Rehabilitation of radicalised and terrorist offenders', pp. 6-7.
[247] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', p. 59.
[248] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', pp.63-64.
[249] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', pp. 65-66.

Beyond outlining a 10-step approach to working with families in any radicalisation context[250], the *Radicalisation Awareness Network* recommends five additional government agency responses to supporting returnees and their families:

- Assess the relationship between the returnee and his / her family and social network;
- Be transparent about information gathering and sharing with authorities;
- Inform the family about the legal consequences of aiding their children;
- Be aware of additional risks to which returnees and their families are exposed;
- Consider the position of the family in the wider community[251].

From this baseline, the Network specifies a series of dedicated measures applying to returnee children, with particular emphasis on 'normalisation' as a guiding principle:

- **Focus on early intervention and normalisation**: States need to begin normalising the day-to-day lives of the children and socialising them into an appropriate social network as soon as possible after their arrival. Children will benefit from a structured 'normal' and safe environment in which they can interact with their peers at school.

- **A holistic, multi-agency approach**: A multi-agency approach is needed to address the personal, family, and social needs of the child, including law enforcement agencies, child services, social care services, local authorities, schools, health services, prison and probation related services (e.g., when parents are in prison), employment services, sports and leisure organisations, religious and charity organisations.

- **A tailor-made approach based on individual risk and need assessment:** each case will have its own background, dynamics, risks, and opportunities for rehabilitation, which should be reflected in a risk and needs assessment[252].

To achieve these aims, France has produced a flow chart to specify each step of a child's return home to their country, with exhaustive guidance as to which institutions have responsibility for each phase and action[253].

In terms of practical application of these measures, particularly in line with best policy and legal practice, Switzerland's C/PVE National Action Plan offers detailed guidance on how multiple government agencies and stakeholders can facilitate whole-of-government approaches to this process. The plan specifies '**Disengagement measures for children and adolescents**' (Measure 21 b))[254] targeting: 'any children and adolescents who are classified as radicalised, irrespective of whether they are involved in criminal proceedings, and regardless of their degree of radicalisation'[255]. Responsibilities are assigned across children and youth services of the cantonal psychiatric clinics, social services, and the education sector.

[250] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', p. 55.

[251] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', pp. 57-59.

[252] Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', pp. 70-71.

[253] 'Guidelines on the support to minors once they return from the Iraqi-Syrian zone', in: Radicalisation Awareness Network, 'Responses to returnees: Foreign terrorist fighters and their families', p. 72.

[254] Swiss National Action Plan, p. 21.

[255] Swiss National Action Plan, p. 20.

Chapter Seven: Communication

Introduction

In line with broader counter terrorism and P/CVE strategies, governments need to prevent terrorist and extremist communications achieving their intended objectives, and, in the process, disrupt terrorist and extremist activity, particularly across terrorists' preferred communication channels, and deny them an audience.

To achieve this outcome, whole-of-society approaches are required to design and disseminate effective counter narratives at local and national levels. Government institutions need to communicate their counter terrorism policies effectively and unambiguously, both as a collective and as individual agencies. Methods for constructing and disseminating effective narratives and necessary counter measures against terrorist propaganda can be adapted to suit day-to-day and time-limited crisis communications. This layered approach offers more opportunities for communications to achieve their intended objectives. However, beyond these requirements, societies also need trusted, objective, and independent media and information sources.

Independent Media

In any democracy it is vital to ensure that the national media sector is independent and shares reliable information. Well-capacitated national and local media, reflecting balance and depth in their reporting, enhance public trust and confidence in news sources.

Government has a key role to play in guaranteeing the existence of a broad range of independent media – whether audio-visual, radio, online, or print media – by ensuring an effective regulatory framework is in place. The framework needs to guarantee freedom of expression whilst at the same time ensuring a balance between this freedom and other issues including, for example, foreign ownership of platforms. Independent regulators are one means of achieving this goal[256].

At the same time, media need to develop sufficient capacity to report effectively on a broad range of issues and to ensure balanced reporting and avoid bias[257]. In broad terms, reporting on counter terrorism and P/CVE is similar to reporting on wider security policies and practices[258]. However, while reporting on terrorism impartially, media need to develop specific skills and approaches to avoid giving terrorists a propaganda platform. Dedicated resources outline best practice for media ranging from ethical, professional, to safety issues[259]. Media need to maintain their independence, their responsibility to the general public, their relations with authorities, ensure their journalism is inclusive, and uphold the rule of law and human rights[260].

[256] For best practice, see, for example, Council of Europe, 'Media Regulatory Authorities', available at: https://www.coe.int/en/web/freedom-expression/media-regulatory-authorities ; and, Council of Europe, 'The Independence of Media Regulatory Authorities in Europe', IRIS Special 2019-1, 2019, available at: https://rm.coe.int/the-independence-of-media-regulatory-authorities-in-europe/168097e504.

[257] See, for example, OSCE, *The Media Self-Regulation Guidebook*, 2008, available at: https://www.osce.org/fom/31497

[258] See, for example, Marina Caparini (ed.), *Media in Security and Governance: The Role of the News Media in Security, Oversight, and Accountability*, 2004, available at: https://gsdrc.org/document-library/media-in-security-and-governance-the-role-of-the-news-media-in-security/

[259] See, for example, UNESCO, *Terrorism and the Media: A Handbook for Journalists*, 2017, available at: https://en.unesco.org/news/terrorism-and-media-handbook-journalists and https://unesdoc.unesco.org/ark:/48223/pf0000247074

[260] UNESCO, *Terrorism and the Media: A Handbook for Journalists*, 2017, pp. 28-39.

Similarly, governments need to ensure that reliable information is shared with the media. This requirement is fundamental to ensure confidence in information routinely issued by government focal points: otherwise trust in government degrades very quickly.

Monitoring

State and society need to monitor a variety of individuals, societal groups, and social media to detect radicalisation processes and platforms. A C/PVE National Action Plan can specify monitoring responsibilities and formats, as well as mechanisms for sharing information. The overall effectiveness of monitoring depends on how proactive citizens and institutions are in detecting signs of radicalisation and sharing them with the wider community, government representatives, and P/CVE focal points. Training is often required so that a broad range of stakeholders can detect radicalisation.

Monitoring at Community Level

At the community level of 'everyday' monitoring, law enforcement, educators, and community groups need to watch for signs of radicalisation, extremist propaganda, or any other radicalisation activities. Monitoring for individuals' or groups' changed behaviours, and the appearance of new types of propaganda, whether graffiti, pamphlets, posters, stickers, any of which might mention specific social media channels, will help define the format for a variety of P/CVE responses including communications and messaging. In the Swiss P/CVE National Action Plan, a broad measure on 'use of early detection instruments' (Measure 7)[261] comprises:

> Experts, specialist agencies, youth welfare offices, social services, child and adult protection authorities, authorities, for the execution of criminal penalties and measures, and police.

Monitoring in Youth and Education

Many countries have introduced monitoring programmes in the education sphere, but tailoring them effectively is important. The overall process is similar to routine monitoring for other types of discriminative or potentially anti-social or criminal behaviour.

Firstly, training needs to be available to orient stakeholders beyond government to detect signs of radicalisation. Per Switzerland's National Action Plan, such training is a top priority. Measure 2 focuses on 'Offers of basic and continuing education and training for a broad range of experts', specifying that, in basic and continuing education and training courses:

> experts discuss the issue of radicalisation and violent extremism, and are made aware of how to recognise the signs and risks of radicalisation at an early stage and to act accordingly in order to prevent increased radicalisation. Experts also learn how to deal with people who may have been radicalised[262].

[261] Swiss Security Network (Sicherheitsverbund Schweiz), *Swiss National Action Plan to Prevent and Counter Radicalisation and Violent Extremism*, 4th December 2017, p. 15, available at: https://www.newsd.admin.ch/newsd/message/attachments/50703.pdf

[262] *Swiss National Action Plan*, p. 13.

Subsequent measures include the same priority: ‘Raising awareness among and providing training for key people’ (Measure 5) states the need to:

> raise the awareness of managers and key people at sports and leisure clubs and cultural associations in relation to the issues of violence prevention, radicalisation and violent extremism and provide related training[263].

Measure 7 on the ‘Use of early detection instruments[264]’ also addresses the need to help specialist government agencies with responsibility for prevention clarify the actual extremist risk to initiate further measures to address them.

The comprehensive approach of these measures targets multiple stakeholders, including, for Measure 2 alone:

> youth and (school) social workers, teaching staff, apprenticeship supervisors in host companies, prison staff, police, intelligence services, adult and juvenile prosecution services, juvenile court judges, asylum and migration authorities, residents’ services, child and adult protection authorities, courts, professional guardians, professional personnel in the armed forces and civil protection services[265].

Measure 5 expands this further to ‘Employees in social and youth work organisations, key people in sports and leisure clubs and cultural associations[266]’, and Measure 7 foresees additional training for key stakeholders already addressed in Measure 2, principally: ‘agencies, youth welfare offices, social services, child and adult protection authorities, authorities for the execution of criminal penalties and measures, and police[267]’.

Secondly, guidance is required on how to share radicalisation warning signals and behavioural indicators. Some countries have produced factsheets to orient education and youth group staff on new radicalisation risks and key indicators to monitor for. The need has prompted ministries to issue joint guidance in line with the cooperative nature of a national P/CVE action plan, and these opportunities have also been used to reiterate points of contact for information sharing.

In the case of the UK, in 2015 the British government produced quick reference briefing notes for use by schools and educators identifying how social media is used to encourage travel to Syria and Iraq[268]. Issued jointly by **Home Office** (the UK **Ministry of Internal Affairs**) and the **Department for Education**, the short factsheet included examples of contemporary Islamic State propaganda imagery and themes (inc. image of success/status and belonging/personal duty/defence of Sunnis), the social media platforms used for extremist communication and propaganda (inc. Facebook, Twitter, YouTube, Telegram and instant messaging services), and language used by Islamic State in the radicalisation discourse (inc. ‘Dawla’, ‘Caliphate’, ‘Umma’, and ‘Mujahid’).

The Note also specifies the action schools and teachers need to take, including discussion with a dedicated ‘safeguarding’ focal point who can contact official extremist prevention programmes (in the case of the UK, the ‘Prevent’ extremist monitoring and associated deradicalisation ‘Channel’ programmes), contact the local police force, and direct discussion with the ‘Channel’ programme itself. This comprehensive approach reflects the severity of the challenge the UK has faced in preventing children and youth

[263] *Swiss National Action Plan*, p. 15.

[264] *Swiss National Action Plan,* p. 15.

[265] *Swiss National Action Plan*, pp. 13-14.

[266] *Swiss National Action Plan*, p. 14.

[267] *Swiss National Action Plan*, p. 14.

[268] Home Office and Department for Education, ‘Briefing Note for Schools: How Social Media is used to encourage Travel to Syria and Iraq’, July 2015, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

leaving to join IS. The note also outlines the statutory (legislative) basis for following these recommended procedures.

On the basis of lessons learned, the UK Department for Education has also addressed the issue of improving and intensifying the interaction of local authorities with schools and teachers on radicalisation issues (principally councils responsible for provision of secondary education/senior school), outlining six priorities for effective intervention:

- Agree who is responsible for responding to radicalisation;
- Recognise the need for local authorities to reach agreement about the most appropriate response for them;
- Define a single referral process;
- Build an evidence base;
- Share learning about appropriate interventions;
- Engage with communities to build awareness and understanding[269]

These key priorities remain applicable across other European nations.

Online Monitoring – Mass Observation & Key Channels to Monitor

New forms of non-intrusive online monitoring are available to government institutions. Human resources are still crucial to aggregate information received on new extremist channels, whether from experts, youth workers, educators, or law enforcement. As social media channels are instrumentalised for terrorist recruitment, opportunities exist to automatically detect 'hate speech' used in radicalisation processes, with some methods already having over 80% accuracy[270]. The Global Internet Forum to Counter Terrorism's 'Working Group on Content-Sharing Algorithms, Processes, and Positive Interventions' shares algorithms and processes to identify risk mitigation and opportunities for positive interventions, while countering the consumption of specific content that could increase user interest[271].

The proliferation of social media channels has allowed terrorist groups to 'flip' between different providers to communicate different types of messages, whether focused on violent images and propaganda, or longer form written texts, all of which allow propaganda to be communicated until such time as a channel is closed by a provider.

Facebook, Twitter, YouTube, and Telegram have all been popular amongst extremists at various times, with Telegram – like WhatsApp – serving a coordination function. Telegram has proved particularly useful as many extremist channels are not blocked, key channels also have mirrors on the same service as a hedge against their removal, and some channels also promote content on Twitter, Facebook, and Instagram[272]. These flexible approaches have not been used by other less effective extremist movements. For example, the Parler app was used by North America extremists to prepare the ground for and then implement the coordinated terrorist attack on the US Capitol in January 2021. The Parler app also publicly leaked multiple layers of data allowing federal and state level law enforcement to geo-locate every Parler user present at the attack on the Capitol. These actions ultimately led to Parler's temporary removal from

[269] Thomas Chisholm and Alice Coulter, Kantar Public, 'Safeguarding and radicalisation', Department for Education, *DoE Research Report*, August 2017 available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635262/Safeguarding_and_Radicalisation.pdf

[270] Tom De Smedt, Guy de Pauw, and Pieter Van Ostaeyen, 'Automatic Detection of Online Jihadist Hate Speech', *Computational Linguistics & Psycholinguistics CliPS Technical Report Series*, CTRS 007, February 2018, available at: https://www.academia.edu/36127816/Automatic_Detection_of_Online_Jihadist_Hate_Speech

[271] GIFCT, 'Working Group on Content-Sharing Algorithms, Processes, and Positive Interventions', available at: https://gifct.org/working-groups/

[272] See, for example, Laura Smith, 'Messaging app Telegram centrepiece of IS social media strategy', *BBC Monitoring*, 5th June 2017, https://www.bbc.com/news/technology-39743252

Android and Apple platforms, along with the loss of its Amazon hosted servers.

Hence, although there is a perception that successful use of social media by an armed group results in a global brand and international attention, most armed groups successfully use social media at local and regional levels, escaping monitoring by western nations and the owners of social media platforms. Social media use varies significantly between armed groups within the same conflict, and also varies among different conflicts. Further, the social media platform most used by armed groups also varies between conflicts, reflecting pre-conflict conditions and differences in platform policies[273]. Consequently, states have to be ready to monitor multiple social media platforms in different contexts.

Counter-terrorist and P/CVE professionals monitoring extremist communications can benefit from the proliferation of open-source investigation organisations and specialists who monitor a variety of social media channels for information on new developments in conflict zones. Although these include some focused only on state activity[274], some individuals comprehensively monitor radicalisation and extremist networks in real time[275]. In the absence of an international tribunal for Syria / Syria-Iraq some journalists also release useful information detailing exhaustive IS membership records and data from phones and memory cards that can be used for prosecution purposes as much as in formulating counter narratives[276].

Online Monitoring – Surveillance and Interception of Communications and Bulk Data

In terms of more intrusive monitoring related to suspicions of individuals' involvement in terrorism, any surveillance component needs to be in line with international and European best practice outlined in Chapter Two's 'Policy and Legal Challenges' section. As a broad guide, the initiative 'about:intel' at the non-profit Stiftung Neue Verantwortung collates contemporary guidance on surveillance law, bulk collection of data, and interception of communications[277].

Online Monitoring – Combining Approaches

Due to the current proliferation of influence operations in the United States, the importance of building a multi-stakeholder community to monitor many types of influence operations is now seen as a crucial first step towards countering misinformation and propaganda that drives a variety of anti-democratic extremist activities. Countering influence operations requires not just data from companies and collaboration among researchers[278], but also inputs from policymakers themselves[279]. This approach foresees the creation of a multi-stakeholder research and development centre (MRDC) as an independent venue where tech industry and external researchers can come together for a sustained period to collaborate on monitoring and programming issues within a common structure: in the words of the founder, the MRDC

[273] Laura Courchesne and Brian McQuinn, 'After the Islamic State: Social Media and Armed Groups', *War on the Rocks*, 9th April 2021, available at: https://warontherocks.com/2021/04/after-the-islamic-state-social-media-and-armed-groups/

[274] See, for example, https://www.bellingcat.com and https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/.

[275] See, for example, https://twitter.com/p_vanostaeyen, https://twitter.com/ajaltamimi , and https://www.twitter.com/lindseysnell

[276] See, for example, Jenan Moussa's publication of the ISIS Files in November 2020, available at: https://twitter.com/jenanmoussa/status/1329421535900291073?lang=en ; also see Jenan Moussa's investigation into Omaima A., a German citizen who travelled to Syria, married a terrorist, and then returned to Germany after working as a recruiter for IS: 'Widow of prominent IS terrorist reportedly living quiet life in Germany', *Deutsche Welle*, 16th April 2019, available at: https://www.dw.com/en/widow-of-prominent-is-terrorist-reportedly-living-quiet-life-in-germany/a-48357266

[277] See: https://aboutintel.eu/

[278] Kelly Born, 'Building a community to counter influence operations: Four questions for Alicia Wanless ', *Hewlett Foundation*, 29th March 2021, available at: https://hewlett.org/building-a-community-to-counter-influence-operations-four-questions-for-alicia-wanless/

[279] See, for example, Carnegie Endowment for International Peace, 'Partnership for Countering Influence Operations', available at: https://carnegieendowment.org/specialprojects/counteringinfluenceoperations

is ‘more than a vehicle for data sharing, but a bridge organization that can vet researchers, address contracting issues, and sustain longer-term research projects’[280].

Countering Disinformation

The challenge of countering disinformation in the age of social media is significant, and complicated by the reprise of state-level ‘active measures’ to promote disinformation across media platforms[281]. Government needs the capacity to clearly communicate the objectives of all security policy, whether threat levels determining policy, or key public security priorities, as well as the particularities of a P/CVE campaign.-

Even if citizens are sufficiently educated to discern false or misleading information, a five-step approach can limit the impact of disinformation and disrupt its effectiveness, comprising: the availability of reliable information; clarity of government policy objectives; uncontroversial institutional practices; active countering of disinformation narratives; and reaction to crises with reliable information.

As discussed in the first section, the principal element of countering disinformation is to ensure that the national media sector is independent and shares reliable information. If the media sector is trusted to supply balanced information, then confidence in and the credibility of the media is enhanced across society.

Secondly, government needs to ensure that counter-terrorism and counter extremism policies are clearly understood by the general public, and that institutions follow the policies. This approach limits any ambiguity over the objectives of state policy that extremists can exploit. The same principle feeds into the third step of ensuring that government’s security providers abide by best practice when implementing policy: any missteps or controversial actions can feed grievances that extremists can exploit within society.

Fourthly, disinformation and propaganda need to be actively countered. Institutions need to proactively identify and flag disinformation. By monitoring sources of disinformation or radicalisation narratives, particularly on social media channels, governments have an early opportunity to formulate a public response that disrupts the propaganda’s impact. Government and other stakeholders need to construct narratives that emphasise the costs, illegitimacy, and lack of credibility of extremist narratives. In parallel, governments need to avoid allegations of arbitrary censorship. Striking an appropriate balance can be difficult in extreme circumstances, but this challenge is essentially the same as others faced in crisis management situations. Remedies such as time-limited information sharing restrictions may be necessary in extraordinary circumstances.

Finally, as with any response to terrorist activity in general, in crises it is crucial that government cite reliable sources and reliable media. Failure to share reliable information can damage credibility and trust and undermine other strategic responses to extremist activities. At the same time, in countering propaganda, governments need to be careful to avoid accusations that they are creating propaganda themselves[282].

Overall, governments need to be proactive in their communication, particularly strategic communications, on P/CVE issues. By identifying the nature of terrorist threats, outlining the types of risks, and elaborat-

[280] Kelly Born, ‘Building a community to counter influence operations’, 29th March 2021.

[281] For examples of Russian disinformation, see, for example: Reuters Staff, ‘German Government Accuses Russian media of biased reporting’, *Reuters*, 19th February 2016, available at: https://www.reuters.com/article/germany-russia-media-idINL8N15Y3H3 **;** Stefan Meister, ‘The "Lisa case": Germany as a target of Russian disinformation’, *NATO Review*, 25th July 2016, available at: https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html ; Mark Galeotti, ‘Controlling Chaos: How Russia Manages its Political War in Europe’, *ECFR Policy Brief*, 1st September 2017, available at: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/ ; Jeffrey Mankoff, ‘Russian Influence Operations and Germany and Their Effect’, *CSIS Commentary*, 3rd February 2020, available at: https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect

[282] For an example of a controversial approach to countering jihadi propaganda, see: Piers Robinson, ‘The British government has already forgotten the great dangers of propaganda’, *The Guardian,* 3rd May 2016, available at: https://www.theguardian.com/commentisfree/2016/may/03/british-government-propaganda-counter-terrorism-muslim-communities

ing the national strategic response to terrorism, confidence can be created in the national approach to the problem. Ambiguity or lack of communication creates an information vacuum in which public trust is quickly degraded.

Messaging & Credible Counter Radicalisation Narratives

Disrupting terrorists' messaging, propaganda, and narratives offers a way to degrade terrorist groups in both the short and long term. However, creating credible counter radicalisation narratives remains a significant challenge. Although there are examples of effective frameworks to refine counter narratives and messaging, examples of bad practice tend to outweigh those of good practice. The key need is to ensure the credibility of messaging and messengers, a need that also affects Crisis Communications addressed in the next section.

Ineffective and inconclusive campaigns

The Royal United Services Institute (RUSI) has highlighted the lack of data documenting both the effectiveness of counternarratives and their achievement of intended outcomes[283]. Out of a recent sample of nine counternarrative projects in western Europe, only one achieved a limited output, and none were measured as successful[284]. Some studies list quantitative findings but these are often based on 'vanity metrics' including 'reach, views, and engagement' online statistics that that give no insight into cognitive, attitudinal or behavioural shifts, or the offline conduct of audiences[285]. While advances have been made in social media analytics, methods to systematically measure the influence of interventions remain subjective, abstract, and largely unverified[286]: these criticisms reinforce the need to carefully design communications and identify credible messengers who can demonstrably change a target group's behaviour.

Miscommunication risks

Beyond ineffectiveness, badly designed campaigns can have unintended consequences. In elaborating their GAMMMA+ model, the Radicalisation Awareness Network have identified several examples of what can go wrong in a communications campaign, including: reinforcing conspiracy theories; getting the wrong answers from surveys; campaigns becoming invisible; and using the wrong medium (particularly on social media) to engage target groups[287].

The risk of campaigns backfiring remains constant. A typical risk is that making people, and youth in particular, aware of something that authorities consider inappropriate or harmful, such as drugs, may generate (more) interest in the issue instead of dissuading them[288]. Consequently, alternative narratives and counter-narratives have to anticipate a number of cultural, social, and qualitative issues to ensure a minimum of credibility[289].

[283] Michael Jones, 'Through the Looking Glass: Assessing the Evidence Base for P/CVE Communications', *RUSI Occasional Papers*, 17th July 2020, p. 6., available at: https://rusi.org/publication/occasional-papers/through-looking-glass-assessing-evidence-base-pcve-communications

[284] Michael Jones, 'Through the Looking Glass', *RUSI Occasional Papers*, p. 6.

[285] Michael Jones, 'Through the Looking Glass', *RUSI Occasional Papers*, p. 6.

[286] Michael Jones, 'Through the Looking Glass', *RUSI Occasional Papers*, p. 6.

[287] Alexander Ritzmann, Lieke Wouterse and Merle Verdegaal, 'Effective Narratives: Updating the GAMMMA+ model – (Ex Post Paper from the RAN C&N Academy 'How to create, implement and evaluate an effective P/CVE communications campaign)', 14-15 November 2019, Brussels, *Radicalisation Awareness Network*, 19th December 2019, p. 3, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-c-and-n/docs/ran_cn_academy_creating_implementing_effective_campaigns_brussels_14-15112019_en.pdf

[288] Ritzmann, Wouterse and Verdegaal, 'Effective Narratives: Updating the GAMMMA+ model', p. 13.

[289] Ritzmann, Wouterse and Verdegaal, 'Effective Narratives: Updating the GAMMMA+ model', pp. 13-16.

Best practice – general principles

The European Parliament's general policy recommendations on strategic counter-terrorism and P/CVE issues outline a best practice framework focused on disrupting terrorists' messaging objectives[290] which also feeds into the GAMMMA+ model for developing specific messaging campaigns. The key elements of the framework are:

- **Disruption Activities** Disruption needs to be applied comprehensively and across multiple platforms to avoid displacing terrorist messaging activity to other channels. The vacuum created by disruption needs to be filled with messages designed to resonate with the target audience.
- **Campaign & Message Design** To ensure coherent messaging, campaign and message design principles need to be synchronised through the establishment of a clear and simple-to-understand central narrative, which is supported by a thematically diverse array of messages.
- **Target Audience** Clearly identify the target audience and take into account a spectrum of potential consumers of the message (intended, unintended, supporters, adversaries, and neutrals). A nuanced understanding of potential audiences is needed to persuasively shape attitudes and behaviours.
- **Metrics & Evaluation** Assess the strategic literacy, technical literacy of target audiences to establish a baseline measure against which to measure the impact of messaging. Monitor the effectiveness of the campaign against this baseline.
- **Synchronisation with Action** To gain trust, credibility, or legitimacy in the eyes of a target audience, messaging needs to be synchronised with operational activities on the ground in order reduce any disparity between what a government or institutions say and do (the 'say-do' gap). The central requirement for improving the synchronisation of messaging and action across bureaucracies is largely cultural.

Best practice – organisational level

In terms of organisational best practice, the International Centre for the Study of Radicalisation (ICSR) advice on design and thematic content can further refine the synchronisation of institutions' collective and individual messaging.

- **Monitoring and Evaluation (M&E) Matters**: Monitoring and evaluation metrics are crucial commodities in counter-extremism work. Systematise M&E and make the efforts visible to the public as an exercise in transparency.
- **Be Creative**: Focal points and activists should be imaginative when thinking about developing counter-speech campaigns. Unusual and clever campaigns invite audience participation and have a greater tendency to go viral – while not strictly necessary to all counter-speech efforts, they almost always bolster campaign potential and reach.
- **Think Obliquely**: Activists must always try to think outside of the box. Counter-speech activism often limits itself to providing direct responses to claims made in extremist propaganda. While important in their own right, campaigns that are strictly reactive are only effective to a limited extent.
- **Calibrate Carefully**: Good counter-speech is targeted counter-speech. While it may be tempting to cast the net as widely as possible with a given campaign, doing so is rarely a good idea. Instead, activists and organisations alike should make an effort to calibrate their activities as carefully as possible.
- **Don't Overcomplicate**: No counter-speech campaign has the ability to singlehandedly solve the manifold challenges presented by extremism. Through simple structuring and realistic targeting, counter-speech activists and organisations can work together in unison, offering the holistic response required to challenge extremism meaningfully and systematically across the spectrum[291].

[290] European Parliament, 'Countering Terrorist Narratives', *European Parliament LIBE Committee*, Study PE 596.829, November 2017, pp. 39-42, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/596829/IPOL_STU(2017)596829_EN.pdf

[291] Charlie Winter & Johanna Fürst*, Challenging Hate: Counter-speech Practices in Europe, ICSR*, 2017, available at: https://icsr.info/wp-content/uploads/2018/03/ICSR-Report-Challenging-Hate-Counter-speech-Practices-in-Europe.pdf

Best practice - detailed messaging guidance

The EU Radicalisation Awareness Network's EU GAMMMA+ outlines a detailed methodology for creating effective campaigns. The **GAMMMA+** model has served practitioners from all over the European Union as a tool when planning and implementing communications campaigns[292] and breaks down each step across the messaging cycle into identifying the intended: **Goal**; **Audience**; **Message**; **Messenger**; **Medium**; **Action**; and **Monitoring**. The comprehensive step-by-step methodology outlines common errors to avoid[293]. The Radicalisation Awareness Network's Communication and Narratives Working Group has also collated a wide range of messaging campaigns and samples of counter narratives and identifies lessons learned[294].

At a national level, mainstreaming credible counter-radicalisation narratives into national policy requires a coordinated whole-of-society approach. To achieve this common goal, one example is Switzerland's National Action Plan which has a measure dedicated to counter narratives and alternative narratives. Measure 20 addresses '**Prevention of radicalisation, in particular via the Internet, by means of counter narratives and alternative narratives'** with the rationale that people who look for or come across violent extremist propaganda on the internet must be able to find other perspectives and counter arguments in order to keep a critical distance and to build a positive identity. The Measure states that the approach must go beyond government institutions and agencies, specifiying that:

> the development and dissemination of counter narratives and/or alternative narratives on the internet and offline is supported by initiatives in civil society and includes as many people in the target group as possible[295].

In this way, the development of credible counter narratives is situated in a comprehensive whole-of-society approach to P/CVE.

Crisis Communications

Communications during – and in the immediate aftermath – of a terrorist attack need to be reliable and also reassure the population. Achieving these two objectives disrupts the terrorists' intended aim of creating fear amongst the population.

For media outlets and reporters there are ground rules to follow to avoid amplifying the terrorists' actions. The UNESCO handbook for journalists on 'Terrorism and the Media' breaks down relevant guidance for media into: objective coverage of the attack itself; sifting through the initial confusion for reliable data; preparation of reports; and the process of live broadcasting from the scene of the attack[296].

States need to develop the capacity to respond to terrorist attacks in real time and to clearly communicate with, also reassure, the general public. Guidance includes the EU funded SAFE-COMMS crisis manual that still provides a useful structure for institutions to approach crisis communication subsequent

[292] Ritzmann, Wouterse and Verdegaal, 'Effective Narratives: Updating the GAMMMA+ model', *Radicalisation Awareness Network*, 19th December 2019, pp. 1-12.

[293] Ritzmann, Wouterse and Verdegaal, 'Effective Narratives: Updating the GAMMMA+ model', *Radicalisation Awareness Network*, 19th December 2019, pp. 3-12.

[294] Radicalisation Awareness Network, 'Preventing Radicalisation to Terrorism and Violent Extremism: Delivering counter- or alternative narratives', *RAN Collection of Approaches and Practices*, 2019, available at: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/networks/radicalisation_awareness_network/ran-best-practices/docs/delivering_alternative_narratives_en.pdf

[295] *Swiss National Action Plan*, p. 20.

[296] UNESCO, *Terrorism and the Media: A Handbook for Journalists*, pp. 71-74.

to a terrorist attack[297]. The Radicalisation Awareness Network's 'Communication and Narratives Working Group' features continuously updated best practice on its webpage, including video testimony[298]. Additionally, the International Centre for Counter-Terrorism (ICCT) and the RUSI have also identified six key lessons that guide the development of a post-terrorist incident communications response framework:

- Post-incident responses need to be calibrated to 'compete' against malignant actors (such as terrorist propagandists) in an effort to shape meaning-generation processes in target audiences.
- Post-incident guidelines must harness the ecology of crisis communications of which social media is an important, but not the only, component. No medium of communication is inherently positive or negative. Instead, strategies need to be devised to harness its potential positive effects.
- Social media platforms can play a key role in assisting emergency services and, rather than shutting down after a terrorist attack, these mediums can be used to reassure, advise, and inform.
- Social media platforms and media organisations will need to work collaboratively to ensure post-incident reporting frameworks are complementary.
- Social media companies will need to be prepared to remove terrorist content, especially that which is designed to trigger and amplify fear in target audiences, in a timely and appropriate manner.
- Social media platforms can play a significant role in post-incident responses in appreciating and assisting the importance of the online space for bringing communities together in the wake of a terrorist attack as a shared space for grieving and sense-making[299].

In terms of putting these principles into practice, the immediate response of the Belgian Federal Government's Crisis Centre's to the Brussels terror attacks in March 2016 is a useful example of a crisis communications team achieving a positive impact. Notably, the Belgian Federal Government's Crisis Centre (FCC) applied a communication strategy focused on restoring trust by diminishing the victims' and other stakeholders' anxiety and stress levels[300].

To achieve this impact, the FCC's responsible communications support team of thirty people, known as Team D5, used – and were trained on – a **Crisis Communication Work Process (CCWP)[301]** established in 2014 that integrated the **IBSE Framework** into its work, a structure that helped reduce the stress of uncertainty within the communication team itself.

The CCWP focuses on solving four challenges: taking ownership of a crisis; provide strategic advice enriched with relevant information; adapting to the mental thinking patterns and models of the audience; and the difference between communications as a separate discipline from other crisis responders[302]. The CCWP acknowledges the existence of an information vacuum at the start of a crisis and the audience's perception of how a crisis is unfolding. Team D5 also featured a coordinator to interface within the team and with other external communicators involved in the crisis[303], working closely with the FCC communications team, and other institutional communications teams (inc. public transport companies, prosecutor's office) using the CCWP at three levels: communication strategy, tactics, and operations[304].

On the day of the attacks, Team D5 used the **Information, Behaviour, Sensemaking, and Expectations (IBSE) Framework** to analyse conversations posted online on social media and on other public forums.

[297] SAFE-COMMS Consortium, *The Terrorism Crisis Communication Manual for Public Authorities*, EU Seventh Framework Programme (FP7), 2011, available at: https://faculty.biu.ac.il/~sshpiro/crisis_manual.html

[298] RAN Communication and Narratives Working Group (RAN C&N) https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/topics-and-working-groups/ran-c-and-n_en

[299] Alastair Reed and Haroro J. Ingram, 'Towards a Framework for Post-Terrorist Incident Communications Strategies', *ICCT & RUSI Global Research Network on Terrorism and Technology Paper*, No. 12, 20th August 2019, available at: https://icct.nl/publication/towards-a-framework-for-post-terrorist-incident-communications-strategies/

[300] Hugo Marynissen and Mike Lauder, 'Stakeholder-Focused Communication Strategy During Crisis: A Case Study Based on the Brussels Terror Attacks', *International Journal of Business Communication*, 2nd November 2019, pp. 176-177, available at: https://journals.sagepub.com/doi/full/10.1177/2329488419882736

[301] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 179-180.

[302] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 180.

[303] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 180.

[304] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 182.

These conversations were classified in terms of four issues:

- **Information**: Issues that express a need for more information;
- **Behaviour**: Issues that concern what behaviours the stakeholder should adopt. This is what (or not) to do, or how (or not) to behave;
- **Sensemaking**: Issues where stakeholders fail to make sense of what is happening, often expressed as emotional (rather than rational) expressions of concern;
- **Expectations**: Issues that request for updates concerning the situation, which can be used to manage stakeholders' expectations[305].

During the attacks, Team D5 classified incoming information according to the IBSE Framework in an overview the whole team could access[306]. The team's response was then focused on three communication channels:

- Public messages published on social media and on their own web site;
- Direct individual answers to citizen inquiries;
- Questions and answers listings used by the team.

Use of the CCWP method gave the Team a certain feeling of 'control' over the situation. When the Team spotted wrong information in the media, they took the appropriate action by calling a news wire's editor, and proactively contacted the Belgian representatives of Twitter and Facebook for publications of alerts from the crisis centre on the social networks' home pages[307].

A retrospective analysis of Team D5's impact across multiple communication platforms indicates that Team D5 answered the questions that were raised by the public. Expressions of concern from the public received appropriate responses guided by the IBSE Framework, demonstrating that the crisis communications team:

> ... were listening before they communicated, and by doing so they reduced the population's stress level and created trust and credibility[308].

In summary, the Communications Director of the FCC stated that:

> ... the use of the CCWP gave Team D5 the confidence to structure its mission and to handle the communication of this complex emergency situation. The methodological approach helped the team to successfully share coordinated information with the population that met the information needs and resonated to the deep human emotions that existed[309].

In this way, Team D5 had prevented the terrorists from achieving all of their intended goals.

[305] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', pp. 180-181.

[306] See, 'Figure 2. An IBSE overview developed by Team D5 on March 22, 2016' in Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 183.

[307] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 187.

[308] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 188-189.

[309] Marynissen and Lauder, 'Stakeholder-Focused Communication Strategy During Crisis', p. 189.

The handbook is printed within the framework of the project “Enhancing the capacity of Georgia in preventing violent extremism and radicalization”. The project is implemented by GCSD with the financial support of the Norwegian Ministry of Foreign Affairs.

Tbilisi, Georgia

2021