# The globalisation of Countering Violent Extremism policies

## *Undermining human rights, instrumentalising civil society*

By Arun Kundnani and Ben Hayes

# Executive Summary

In the early 2000s, a new form of counterterrorism policy – Countering Violent Extremism (CVE) – emerged, pioneered first in the Netherlands and the UK before spreading to other parts of Europe, the US and eventually the rest of the world. Within a decade, as policies were copied from one state to the next and taken-up by the European Union, United Nations and a host of other international fora, CVE was globalised.

From Finland to the Philippines, CVE policies have been presented as a more liberal, more intelligent, more holistic way of dealing with terrorism than the crude and inflammatory "war on terror". This report indicates, on the contrary, that the globalisation of CVE means the globalisation of another set of alarming problems: harm to human rights and the undermining of civil society. We analyse the frenzied adoption of CVE by policy-makers within institutions of the European Union, the United Nations and the Global Counterterrorism Forum, while the core issues that were present at the birth of CVE in the Netherlands and the UK remain unresolved.

The kinds of actions that have been carried out under the CVE label are varied: engagement and outreach; capacity building and development aid; education and training; messaging and public relations campaigns; surveillance partnerships between policing and non-policing agencies; and targeted ideological interventions on individuals. Much of what is labelled as CVE sounds benign or insignificant. But CVE policies have dramatically widened the range of methods used by governments for countering terrorism and broadened their objectives from investigating terrorist individuals and organisations to regulating the ways that ideologies flow through communities and managing how communities understand their cultural identity. CVE brings a new vocabulary: the term "radicalisation", for example, was not heard in counter-terrorism policy-making before 2004; now it is ubiquitous. And CVE calls for relationships with a far wider set of partnering agencies than other modes of counter-terrorism policy. Around the world, all sorts of professionals, from artists and musicians to theologians and schoolteachers, have been drawn into becoming CVE practitioners.

What CVE policies have in common is that they promise to reduce terrorism by using methods beyond the use of military force and the coercion available under criminal law; they usually also aim to prevent the emergence of terrorism before it has fully emerged in a region, community or an individual, by addressing the underlying factors that give rise to it; and they claim to take a partnership approach to the communities they target. Supporters of CVE policies see them as complementing more conventional, reactive counter-terrorism methods, offering the possibility of a long-term and holistic solution to terrorism. What we demonstrate, however, is that CVE policies are not an alternative to securitization but a means of securitizing a wider range of spheres; they are not an alternative to government coercion but an opportunity for greater surveillance and suppression; and they are not based on genuine partnering with civil society so much as a desire to instrumentalise it.

In particular, the report highlights the following recurring problems with CVE policies:

1. *Vague definitions:* Since CVE policies were first introduced in the Netherlands in 2005, they have been continuously beset by a problem of definition. Policy-makers either leave extremism undefined, define it in multiple, inconsistent ways or define it so broadly that large sections of the population could be counted as extremists. This abject lack of consistent definition provides for the implementation of CVE in ways that are discriminatory, opportunistic or politicized. The most common consequence is a disproportionate focus on Muslim populations and an under-examination of far-Right violence.
2. *Empirical incoherence:* Because CVE policies claim to take a preventative approach that addresses the underlying causes of terrorism, it is essential that they are grounded in a plausible account of the causal mechanisms that lead to terrorism. Unfortunately, CVE policies have largely rested on an unfounded assumption that the main cause of terrorism is the circulation of extremist ideology. Despite there being no empirical studies convincingly supporting the claimed role of extremist ideology, stemming the flow of extremist ideas has become the central CVE policy goal. In the case of CVE policies directed at Muslims, this has meant unprecedented interventions and attempts to manipulate the sphere of religious ideology.

3. *Undermining civil society:* A major strand of CVE policy is the attempt to induce changes in cultural, religious and political attitudes and opinions of targeted communities using civil society as a vehicle for change. This use of government "soft power" aims, ultimately, at a cultural transformation of the identities of the targeted communities – perhaps the most ambitious aspect of CVE policy-making. To this end, CVE policies have involved hiring PR agencies to produce media campaigns and have sought to recruit and fund community representatives who are willing to promote the CVE message. The mini-industry of government-funded CVE entrepreneurs that has emerged has gone on to dominate public debate on a range of topics, side-lining more genuine community voices. Government involvement in these propaganda campaigns is usually kept secret so that the campaigns can appear as spontaneous, grassroots initiatives. The overall result is that civil society is weakened in various ways: dissent is marginalised, transparency stifled, stigmatisation facilitated, secularism undermined and gender stereotypes reinforced.
4. *Expanded surveillance:* A key aspect of most CVE policies is the attempt to develop a surveillance system that can monitor communities for signs of radicalisation and then potentially conduct "soft interventions" with individuals suspected of becoming extremists. CVE surveillance is not aimed at identifying imminent criminal behaviour but at detecting a broad range of indicators of ideological concern; in trying to achieve this, it tends to exploit the information generated in the relationships between non-policing public bodies, such as educational and medical services, and the communities they serve. In doing so, CVE policies tend to introduce security and surveillance norms into all areas of government and undermine trust in public services.
5. *Internet censorship:* CVE strategies have involved the development of ad hoc, "voluntary" arrangements between police agencies and internet service providers and social media platforms that enable extremist content to be censored. As digital media corporations largely defer to government instruction on what counts as extremist, the label becomes a means for governments to carry out extra-judicial censorship of their opponents. Facebook, for example, grants 95 per cent of requests from the Israeli government to close down Palestinian accounts, leading to a significant censorship of civil society organisations, such as the Palestine Information Centre.
6. *Potential for abuse:* One of the biggest concerns about CVE programmes is that the breadth of behaviour that can be considered 'extremist' can be applied to perfectly legitimate political activities such as protests, demonstrations and direct actions. Moreover, when CVE policy-makers emphasise the narrative that there is an ideological and cultural problem in Muslim populations, they give official sanction to the Islamophobic messaging of far-Right movements. As CVE policies have become more entrenched, they have increasingly been used to target environmental protestors, pro-Palestinian groups, democracy activists and social justice activists. This kind of political policing, which is increasingly common in western democracies, has been given a new veneer of legitimacy as CVE policies are embraced by more repressive and authoritarian regimes.
7. *Lack of formal legal and political accountability:* CVE policies tend to be mandated by executive decisions rather than legislative frameworks. This means that policies are implemented through partnerships between state agencies, local government, civil society partners and service providers, with very little formal accountability beyond the state bureaucracy.

The report also tracks the embrace of CVE policies by three key intergovernmental organisations: the EU, UN and the Global Counterterrorism Forum.

## European Union

The EU developed its first iteration of what would become its CVE strategy in 2005, with a limited focus on recruitment by terrorist organisations. Today, it appears to have a comprehensive strategy to combat all forms of what it terms "radicalisation leading to violent extremism". Our research suggests the EU's Security Research Programme will have invested more than €400 million on initiatives related to radicalisation between 2007 and 2020. A further €300 million to fund national-level CVE initiatives is promised by the EU's Internal Security Fund between 2014 and 2020.

This huge investment has been accompanied by a steady widening of the scope of EU CVE policy, with responsibility for countering "extremism" now said to fall on upon European "teachers, staff at universities, social workers, youth workers, healthcare providers, volunteers, neighbours, sports coaches, religious and informal leaders, local police officers". In turn, EU funded projects involving councils, universities, NGOs, religious groups, prisons, police authorities, border authorities and transport networks have proliferated. Yet, despite the huge investment and the vast scope of the EU's CVE policy, particularly since 2014, there is no democratic control whatsoever, scant information on what these projects involve, and no clarity or precision as to exactly what it is that is being countered.

In fact, the European Parliament and well-established civil society organisations with an interest in counterterrorism and human rights have been completely marginalised as the EU's CVE policy has developed. National parliaments have had no say either. Instead, policy development has been outsourced to the EU's "Radicalisation Awareness Network" (RAN), which claims to have bought together over 3,000 policing and other CVE "stakeholders" from across the EU. While RAN serves as a clearing house for policy initiatives that have emerged in key member states, there are no meaningful democratic checks on its activities, the membership of its sprawling network is kept secret, and its operations and logistics are managed by a private company. With next to no-one paying any meaningful attention to how the hundreds of millions of euros of CVE funding is being invested by the EU, there is little prospect of policy coherence or value for money, and every chance that initiatives will be implemented in a manner that jeopardises human rights and undermines the independence and pluralism of civil society.

Since 2015, the EU has also presided over an Internet Referral Unit (IRU) housed in EUROPOL, the EU Police Office, which provides an extra-judicial mechanism for the blocking or removal of extremist content by internet service providers (ISPs) and social media platforms. This means that there is no independent oversight of decisions to remove extremist content, with decisions taken by state agencies, ISPs and social media companies. The majority of extremist content removal referrals are carried out as requested by the IRU and its partners, despite there being no formal definition of extremism to guide this process. As internet censorship reaches a level of support and implementation that would have been unthinkable just a decade ago, the architects of these policies and practices have turned their attention to "artificial intelligence" that will enable content removal to be automated in the coming years. This has huge implications for freedom of expression, and for legal and political accountability, with public access to information about political issues like conflict and terrorism now mediated by entities (and algorithms) that appear squarely incapable of implementing policies in an objective, even-handed manner.

The report suggests that a root and branch review of the EU's CVE policies is urgently required, together with reforms that provide for meaningful democratic control and accountability. In the absence of evidence that CVE policies are effective, or in light of evidence of counterproductive outcomes, such as routine fundamental rights infringements, these policies should be reconsidered or re-designed from the ground-up.

## United Nations

The UN approach to CVE, which came to prominence from 2014, has been shaped and characterised by a longer-term tension within the United Nations framework between the 'hard security' approach of its executive counterterrorism agencies, and the ostensibly more holistic, "root causes" approach of the Secretary-General, UN Development Programme and others. With the UN now mandating and encouraging all nations to adopt CVE policies, the way these tensions play out is crucial.

The 2016 UN Plan of Action to Prevent Violent Extremism issued by the Secretary-General suggests that the creation of open, equitable, inclusive and pluralist societies, based on full respect for human rights and with economic opportunities for all, represents the most tangible and meaningful alternative to violent extremism. It builds upon the "root causes" elements of the UN Global Counterterrorism Strategy adopted a decade earlier, as well as progressive Security Council Resolutions reflecting the UN's values and principles of conflict resolution and self-determination. This includes Resolution 2242, which urges the participation and leadership of women in countering terrorism; and Resolution 2250, which calls for the involvement of young people in decision-making and in the prevention and resolution of conflict.

At the same time, the Security Council has adopted Resolution 2178 on stemming the flow of foreign fighters, which mandates extended surveillance, travel restrictions and harmful counter-radicalisation policies, and a follow-up Resolution 2396, mandating enhanced border security, information-sharing, and yet more surveillance. There is widespread and palpable concern among human rights organisations that these particular Resolutions give carte blanche as far as this repressive, "hard security" agenda is concerned. Meanwhile, the more progressive elements of the UN's strategy have been largely confined to briefings and side events in New York and Geneva.

The Security Council has also essentially replicated the UK and EU programmes of internet censorship and top-down, government-led "counter-narratives", which were incorporated into resolution 2354. The UN Counter-Terrorism Committee Executive Directorate has also orchestrated the formation of the Global Internet Forum to Counter Terrorism, which promises to replicate best practice in forms of internet censorship, including the automation of blocking and take-down.

Nevertheless, agencies like the United Nations Development Programme continue to push the "root causes" agenda, which prioritises efforts to address the conditions conducive to extremism and terrorism over the hard security approach of the Security Council. It has published research that rejects the assumption that extremist ideology is the key factor in producing terrorism, focusing instead on the role of state actions in pushing people to support violence. Based on interviews with 500 members of extremist groups in Africa, it found that, in 71 per cent of cases, the tipping point that led to their recruitment was some form of government action, such as the killing or arrest of a family member or friend.

What remains is a complex and often schizophrenic UN policy framework. The report argues that the more progressive approaches to countering violence that are consistent with the UN's core values of conflict resolution and self-determination must be prioritised and implemented. It is also imperative that national parliaments and civil society engage with the development of national action plans to prevent violent extremism under the mandate of the Secretary-General, and provides a framework for analysis and engagement to this effect (see further below). As with the EU, it is crucial that the international funding and technical assistance emanating from the UN's new CVE policy framework is subject to robust scrutiny and forms of democratic control.

## The Global Counterterrorism Forum

The report also examines the CVE policies of the Global Counter Terrorism Forum (GCTF), an international consortium of states established in 2011 by 29 countries and the EU. It was set up by those states most invested in the 'war on terror' as a way to coordinate international policy-making without having to work through the UN with its perceived bureaucracy and excessive concern for human rights and self-determination.

The GCTF CVE working group held its inaugural meeting in Abu Dhabi in 2012. Since then, it has focused heavily on developing and sharing expertise in counter-narrative and propaganda strategies, with the UK model of CVE prominent in its work. The GCTF has also established the Hedayah Center of Excellence in CVE, also based in Abu Dhabi. The Center has provided an 'expert' vehicle for states to outsource policy development and provides catalogues of CVE policies and projects that states can adopt. With the exception of a single initiative engaging with Colombia, all of the national projects catalogued by Hedayah are aimed at tackling "Islamic extremism".

The GCTF also established the Global Community and Engagement Resilience Fund (GCERF), an "independent public-private partnership" which funds local, community-based CVE projects, with a focus on those local communities which "suffer the most from violent extremism". As with the UN system, this has resulted in something of a schizophrenic approach, with the bottom-up, more holistic approach of GCERF pitted against the top-down, securitised approach of the states. And as with the EU system, there is precious little information available as regards the expenditure, implementation or effectiveness of its initiatives.

With various UN agencies attempting to play a more leading role in the area of CVE, and the Obama administration's support for the GCTF now a thing of the past, its influence is likely to dwindle as states look to anchor their CVE policies in the perceived legitimacy of the United Nations framework.

# A framework for analysis and engagement

Using international human rights law and widely accepted best practice principles for public policy, the report concludes with a series of twelve tests that highlight the issues that should be considered the starting point for the development of CVE policies. If properly considered, these tests can, therefore, help ensure that CVE policies are applied even-handedly, in a non-discriminatory manner that respects the diversity and independence of civil society and public and private sector workers.

## Goals

### i) Legitimacy

Is the framework based on an objective, proportionate and unbiased assessment of political violence in a given territory? Does it address multiple forms of political violence and take all relevant social, cultural and political factors into account? Is it supported by an evidence-based account of the causal mechanisms that give rise to violence and how policy actions can intervene to achieve more peaceful outcomes?

### ii) Rights-based approach

Does the approach put respect for fundamental rights at the heart of the policy? Have human rights groups been consulted and their views taken into account when developing the policy?

### iii) Democratic and judicial oversight

Has the policy been developed and implemented democratically? Are mechanisms in place to review the policy and ensure that it is necessary and proportionate, legitimate and effective? Are CVE practitioners legally and politically accountable for their actions?

### iv) Children's rights

In its engagement with children and young people, does the policy prioritize the fundamental rights and best interests of the child, including the right to family life?

### v) Gender equality

Does the policy actively and meaningfully empower women to shape efforts to reduce violence? Have women played an equal role in the development of policy? Is the policy framed and implemented in ways that do not reinforce gender stereotypes and inequalities?

### vi) Coherence

Where political violence is related to an ongoing military conflict or insurgency, is the approach part of a wider conflict transformation strategy? Are the terms and concepts used in the policy precisely defined, including in relation to one another?

## Pitfalls

### i) Racial and religious profiling

Does the policy disproportionately engage with particular racial or religious populations? Are behaviours or markers associated with particular racial or religious populations treated as indicators of a threat of extremism in a way that leads to racial or religious profiling or suspicion falling on groups defined by race or religion? Does the policy stigmatise whole population groups as collectively responsible for the views or actions of individuals or organisations?

### ii) Intrusions into privacy

Does the policy, or the steps leading to the development of the policy, involve the collection of substantial private information on individuals who are not reasonably suspected of involvement in criminal activity? Does the policy result in the sharing of information collected for the purposes of prevention with national security investigative agencies even where there is no reasonable suspicion of criminal activity?

### iii) Religious discrimination

Does the policy associate particular religious practices, behaviours, and beliefs with a risk of violent extremism and thereby lead to a diminishing of the right to express them, through formal or informal censorship? Does the policy involve or allow for state interventions into the religious life of particular populations in order to promote and empower certain forms of religious ideology at the expense of others?

### iv) Political censorship

Does the policy associate particular political beliefs and ideologies with a risk of violent extremism and thereby lead to a diminishing of the right to express them? Does the policy seek to prevent the circulation of particular political opinions through social engineering, formal or informal censorship? Does the policy create 'thought crimes'?

### v) Secrecy

Are aspects of the policy kept secret from the public in ways that make adequate scrutiny difficult? Is the public denied access to a reasonable degree of detail on how the policy works in practice and who developed it?

### vi) Undermining autonomy

In its engagement with civil society and professional spheres, such as health, education, and so on, does the policy fail to prioritize or actively promote their autonomy and protection of their normative professional values (except in cases where there is evidence of harm to others)?


The Transnational Institute (TNI) is an international research and advocacy institute committed to building a just, democratic and sustainable planet. For more than 40 years, TNI has served as a unique nexus between social movements, engaged scholars and policy makers.

www.TNI.org