ISD | Institute for Strategic Dialogue

Lessons from Extremism Prevention for Countering Hybrid Threats

A Framework for Policy Response

Milo Comerford, Emily Winterbotham, Jakob Guhl, Melanie Smith

Acknowledgments

ISD is grateful for our partners at the Konrad Adenauer Stiftung London and Ireland Office for their support in convening the expert roundtable that informed the development of this paper.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Toronto | Washington DC

www.isdglobal.org

CONTENTS

INTRODUCTION

Across Europe, we are seeing the increasing hybridisation of hostile state threats and extremist violence, presenting a growing challenge to national security. Ranging from harmful online influence operations to the fomenting of violent plots, such hybrid threats are constituting new and emerging pathways for mobilising notably younger target audiences towards dangerous activity, largely enabled through online networks.

There are growing parallels in the ways extremist, criminal and hostile-state actors use online platforms to identify and mobilise young people. Young people may be particularly accessible to recruiters operating through social media and messaging platforms. Documented cases show recruits being offered payment for individual tasks and instructed to provide photographs or videos as proof of completion. This is consistent with terrorism trends in Great Britain and the EU, where young people account for an increasing proportion of terrorism-related arrests. In Great Britain, people aged 17 and under accounted for around a fifth of terrorism-related arrests in 2023, compared with 4 percent in the year ending September 2019. In the EU, people aged between 12 and 20 accounted for almost 30 percent of terrorism-related arrests in 2024.

Extremist and hostile-state actors may draw on some of the same divisive narratives, including antisemitism, misogyny, anti-migrant hostility and conspiracy theories. While extremists engage in such activity within a supremacist ideological framework, state actors can perpetuate these harms both as an end in themselves or to weaponise these divisive issues to facilitate the disruption of democratic societies. Although their motives and structures differ, both may exploit or intensify existing divisions, placing pressure on democratic debate, social cohesion and perceptions of community safety.

There are also important distinctions between state-backed operations and violent extremism. Recent hostile-state operations in Europe have increasingly made use of criminal intermediaries and remotely recruited proxies for surveillance, vandalism, arson and other disruptive activity. These recruits are often untrained and motivated by payment rather than ideology and may be assigned relatively low-complexity tasks. Using intermediaries and expendable proxies can reduce cost and direct exposure, complicate attribution and provide a degree of plausible deniability.

This growing landscape of hybrid threats is directly impacting already stretched security responses. UK Counter Terrorism police are grappling with major increases in state threat cases, now accounting for more than 20 percent of casework, while MI5—the UK's domestic security service—has seen more than 20 potentially lethal Iran-backed plots since 2022. Germany established a Joint Centre for the Defence Against Hybrid Threats in June 2026 to strengthen the country's ability to monitor and respond to the growing numbers of hybrid attacks. Such policy approaches to hybrid warfare are moving increasingly from detection and disruption towards more proactive responses, paralleling the growing recognition over the past two decades of the significance of prevention in countering terrorism.

With these threats growing and capacity limited, it is crucial that European governments learn lessons from the wealth of policy, practitioner and academic insights across these interrelated domains. This paper—which draws on a roundtable discussion with experts from the UK and Germany hosted by ISD and the Konrad Adenauer Stiftung's UK and Ireland Office in June 2026—begins to map out a practical framework for policy responses.

It considers which parts of government are best placed to address these threats. It additionally examines the substantive legal distinctions guiding efforts to address state and non-state threats, and their implications for effective joined up responses. And lastly it explores how to build durable and flexible whole-of-society prevention approaches in the context of a fast-evolving threat.

CASE STUDIES: IRAN AND RUSSIA

Iran: 'Islamic Movement of the Companions of the Right'

Between March and April 2026, a previously obscure group describing itself as Harakat Ashab al-Yamin al-Islamiya (The Islamic Movement of the Companions of the Right) claimed responsibility across Europe and Canada for a wave of arson attacks, drive-by shootings at embassies, and a stabbings attack, primarily targeting Jewish (as well as Iranian dissident) communities.

The group, which ISD analysis showed functioned as a 'ghost proxy'—established purely for the purpose of claiming attacks—was allegedly the brainchild of Muhammad Baqer al-Saadi, a high-ranking member of Katai'b Hezbollah, an Iranian Revolutionary Guard Corps (IRGC)-backed Iraqi militia group with a history of launching attacks on US diplomatic and military installations in the Middle East. Al-Saadi, who was close to IRGC leadership, was arrested at an airport in Turkey and transferred to American custody, having called Ashab al-Yamin "our people" and taken credit for attacks in Europe and Canada, while allegedly planning attacks in the US.

The Islamic Movement of the Companions of the Right has used Snapchat to communicate via third-party interlocutors. They organised for unwitting assailants to conduct attacks on targets, turning to organised criminal networks to carry out planned attacks. The strategy follows a pattern seen in previous Iran-linked attacks and plots in Western contexts, including the use of criminal networks to conduct 'violence-as-a-service' attacks in Europe. Iran has previously been linked to criminal networks in Sweden, the United Kingdom, the United States, and Canada.

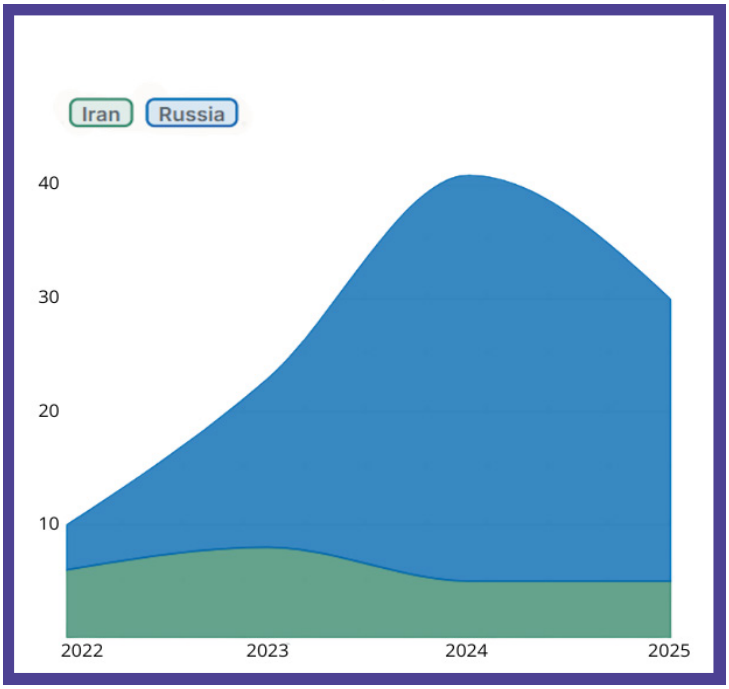
Russia: Wave of Kremlin-linked Hybrid Attacks Across Europe

The Kremlin has long been a pioneer of hybrid warfare targeting Europe. At the time of writing, ISD's Authoritarian Interference Tracker documented 188 incidents linked to Russia targeting democracies across Europe and North America since Russia's full-scale invasion of Ukraine in February 2022. Authorities say that 1,100 Ukrainians have acted as Russian proxies in such incidents, engaging in activities such as sabotage, arson or bombings (i.e. state-orchestrated violence-as-a-service). Of these 1,100, around one in five (240) were minors; most were financially motivated and around half were unemployed, with many recruits seemingly unaware they were working for Russia.

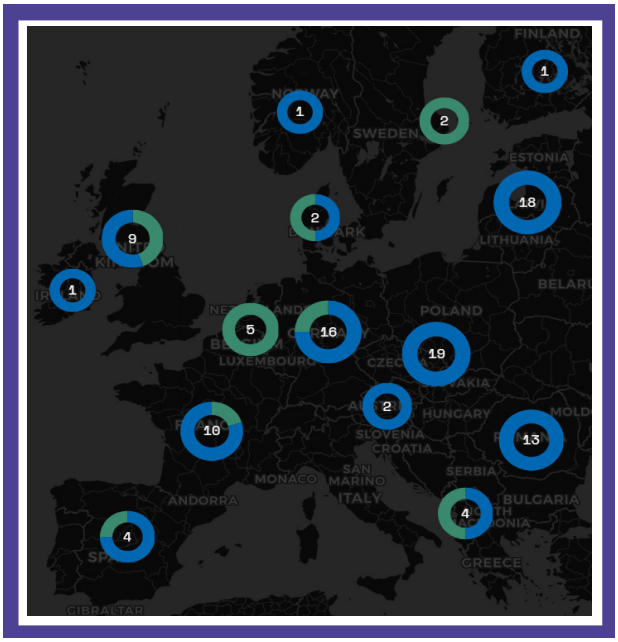
In one recent UK case, a 22-year-old Ukrainian construction worker living in London was convicted of carrying out a series of arson attacks in May 2025 targeting properties linked to former UK Prime Minister Sir Keir Starmer. Evidence presented at trial showed that Lavrynovych had been recruited via Telegram by a Russian-speaking handler who spent months tasking him with low-level activities, including distributing propaganda and graffitiing anti-Muslim slogans. The handler allegedly offered payment in cryptocurrency and was found to be closely aligned with pro-Kremlin hacktivist networks. Investigations also uncovered links between the operation and online influence campaigns designed to inflame social tensions in the UK. The case highlights the growing convergence of extremist and hybrid threats, with foreign actors exploiting extremist narratives to amplify societal divisions and advance strategic objectives.

The following visualisations draw on data from ISD-US' Authoritarian Interference Tracker (AIT), filtered for publicly documented incidents of kinetic activity in Europe linked to Russia and Iran between 2022 and 2025. You can explore the interactive open-source dashboard here.

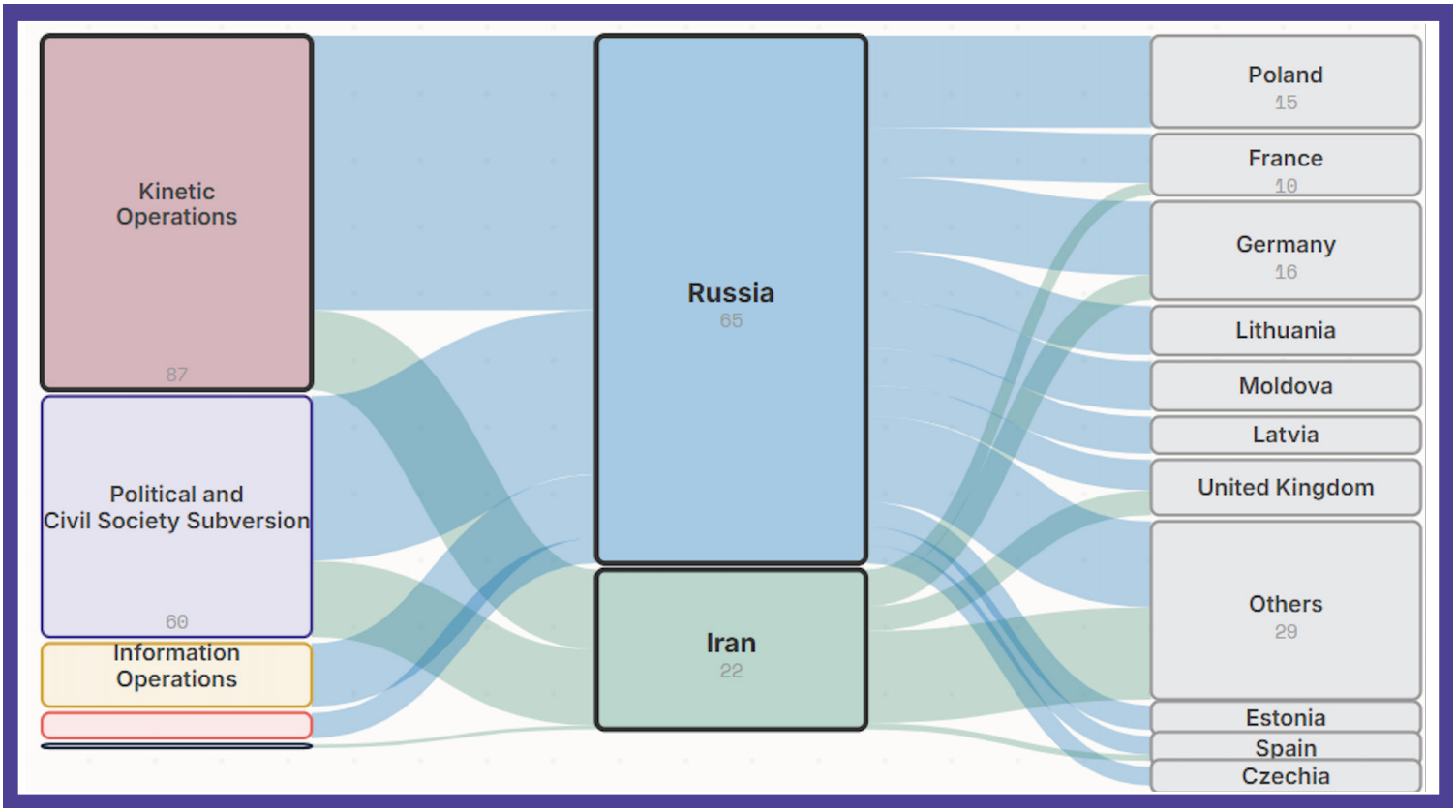
Volume Over Time · by threat actor



Geographic Distribution · by actor share



Incident Flow · type > actor > target country



LESSONS FROM TWO DECADES OF COUNTER-EXTREMISM

Rooting Responses in a Whole-of-Government Approach

At times, counter terrorism (CT) efforts have suffered from being siloed within particular parts of government, resulting in overly securitised approaches that ignore the importance of joined-up, cross-government political strategies for effective prevention. In particular, the false dichotomy drawn between 'foreign' and 'domestic' threats risks hampering coherent government responses to these deeply connected domains.

In the context of this evolving threat, it will be important to consider afresh what a strategic cross-government democracy protection capability might look like and how it could better connect counter-extremism efforts with responses to hostile state threats. Germany offers one model from which lessons might be drawn. Its concept of a 'defensive democracy' provides a common framework for addressing activity that threatens the free democratic basic order, while the remit of its domestic intelligence service encompasses both extremist threats and hostile-state activity. Germany's constitutional and institutional arrangements differ significantly from those of the UK, meaning the model cannot be directly replicated. However, it raises useful questions about whether a stronger democracy protection framework could provide greater coherence across currently separate areas of UK prevention policy.

There is considerable expertise within national security and foreign policy departments on the tactics, tools and techniques employed by hostile state actors. In the UK, this expertise already contributes to cross-government operational responses. However, as the Rycroft Review identified, responsibilities remain dispersed and the continued division between domestic and international functions can hamper a coherent response, particularly when assessing the impact of hostile-state activity on domestic audiences. Strengthening coordination at the prevention level could help governments draw more effectively on existing expertise in areas such as strategic communications, online threat monitoring and audience analysis.

Ensuring Responses are Coordinated Across National and Local Government

Local governments are critical but under-utilised actors in responding to hybrid threats, often bearing the direct impacts of violence and community polarisation. They are closest to communities, meaning that they often have a strong understanding of local needs and potential flashpoints, while also being able to mobilise relevant local stakeholders and groups through existing networks. Moreover, local governments are responsible for providing public services that are crucial for identifying, preventing and responding to community-level challenges, making them particularly well positioned to counter the diffuse and fast-moving nature of hybrid threats. Over a decade of prevention programming, ISD's Strong Cities Network shows how local authorities are uniquely placed to drive social cohesion and community resilience efforts, as well as delivering targeted prevention initiatives that are informed by local dynamics. This includes bringing communities together through shared initiatives and supporting grassroots programming, co-designed around the needs of residents.

The effectiveness of these responses depends on strong national-local cooperation, as highlighted in resources such as the Global Counter-Terrorism Forum's 'National-Local Preventing/Countering Violent Extremism Cooperation Good Practices'. Hybrid threats frequently cut across different policy domains, likely requiring coordinated approaches to information-sharing, resource allocation and programme delivery. Combining national frameworks that set policy direction, resources and responsibilities with local policy agendas, context and implementation that leverage partnerships with local authorities and communities can contribute to the development of mechanisms that can prevent and mitigate hybrid attacks, as well as help communities recover in the wake of them.

The Importance of Policy Responses Focused on the Digital Information Ecosystem

It will be important that efforts to mitigate the digital dimensions of hybrid threats address the role of online platforms across the entire lifecycle of harm—from production to consumption to dissemination. This lesson was learned the hard way in the CT field, with policy efforts

to counter terrorist use of the internet gradually shifting over a decade from reactive removal of terrorist content towards approaches focused on preventing abuse of platform systems and curbing algorithmic amplification and monetisation by harmful networks. However, it should be noted that such efforts still face challenges in being effectively implemented.

Although terrorist and state-linked actors may use some of the same platforms and amplification techniques, the associated risks can differ. Counterterrorism responses have often focused on terrorist propaganda, recruitment material and operational content, while responses to state-linked manipulation must also address deceptive coordination, concealed attribution and the artificial amplification of narratives. This presents different risk profiles when considering the role of platform systems: concerns around terrorist content focus on the inherently harmful impact of exposing audiences to terrorist material, while concerns around state actors place greater emphasis on (exaggerated) popularity and reach. Here, the lack of transparency around online environments (for example their algorithmic architecture) presents a fundamental challenge to regulation, further complicated by Generative AI's lowering of the barrier of entry to producing harmful content. Greater access to publicly available platform data—in line with emerging online harms legislation in the EU and the UK—is essential for researchers and civil society organisations to better understand online ecosystems related to hybrid threats and to support evidence-based policymaking.

As hybrid threat actors increasingly exploit social media and use encrypted messaging platforms and other online channels to recruit and coordinate hostile activity, governments need to strengthen their open-source intelligence (OSINT) capabilities to detect and attribute influence operations. Closer collaboration between government and civil society organisations, as well as creating better mechanisms for sharing intelligence and research on emerging online threats, could complement improved government capacities. Recent cases, including the arson attacks on properties linked to former Prime Minister Keir Starmer, illustrate how online platforms can be used to recruit proxies and coordinate low-cost operations. A BBC investigation linked the alleged Telegram handler behind the attacks to a Russian diplomat and wider pro-Kremlin networks, although Russian state direction was not formally established through the court proceedings

There are also likely lessons from digital counter-terrorism efforts around the need to move beyond platform-by-platform responses and instead address broader online ecosystems of harm. The Global Internet Forum to Counter Terrorism (GIFCT) sets out to provide a cross-platform community of support to prevent repeat transgressive activity across platforms, a mechanism that does not yet exist for state-based inauthentic activity (similar initiatives will likely be required for AI companies). Instead, responses to manipulative state actor activity to date have relied upon the willingness of tech companies to disclose such behaviour on their platforms, with decreasing incentives to do so.

Centring International Collaboration by Default

The highly transnational nature of the hybrid threat picture will require the development of joined-up systems for international responses. This includes coordinating more aligned policy approaches across like-minded European and Five Eyes partners facing related threats. The case of varied terrorist group proscriptions between allies seems to have so far been replicated in the hybrid threats domain, for example in the so-far inconsistent approaches to designation of state actors like the IRGC. Despite many divergences in approach, it is notable that the 2026 US counter-terrorism strategy commits to working closely with partners in Europe to "jointly counter covert state action that looks like terrorism". At the same time, there is emerging cooperation on a European level, with the EU developing integrated approaches through initiatives such as the Knowledge Hub on Prevention of Radicalisation and working groups examining foreign influence, financing and hybrid threats, including prioritising anticipatory tools.

There may also be important lessons from counter-terrorism for developing effective mechanisms for international cooperation. While existing multilateral systems—such as the EU, UN and GIFCT—play an important coordinating role in the CT (counter-terrorism) field, there were often requirements for additional partnerships for more active joint working, agile operational investments, and flexibility to partner needs. The development of more bespoke structures, such as the Global Coalition Against Daesh, provides examples of parallel institutions established with a clear mandate for responding to specific international coordination needs. Outside of more formal multilateral mechanisms, frameworks like the Christchurch Call showed the potential power of voluntary commitments in addressing

the growing international threat from far-right terrorism, which may be relevant models in the context of hybrid threats.

Addressing Wider Harms Beyond the 'Sharp Tip' of Violence

Efforts to counter extremism have often narrowly focused on the sharp, violent tip of the threat. But while protecting national security and public safety are crucial, ISD has long argued there is an urgent need to address the broader impact of extremist mobilisation, for example on human rights and social cohesion. A similarly contextualised approach is required in response to the wider impacts of hybrid threats. For example, authoritarian state-backed threats, abuse, intimidation and harassment of democracy activists in exile can create a chilling effect within diaspora communities and undermine freedom of expression. Similiarly, state-propaganda and influence operations can promote divisive narratives which undermine cohesion within and between communities.

Any response to the growing challenge posed by hybrid threats should therefore consider both upstream and downstream measures—as has been seen in the CT field. A comprehensive counter-hybrid approach will want to avoid duplicating the siloed division between counterterrorism and counter-extremism initiatives that has at times developed over the past 25 years, despite increasing efforts by European governments at integrating these agendas. Instead, both national security threats and challenges to human rights and social cohesion need to be understood as a continuum of harmful activities.

So far, efforts to counter state-linked hybrid warfare have predominantly focused on strengthening resilience to the cognitive appeal of authoritarian propaganda. But the cognitive threat is just one side of the coin; as the recent series of Iran-linked attacks on Jewish communities and Russian-linked arson attacks demonstrate, kinetic activities remain a core part of the hybrid toolkit, highlighting the need for responses that go beyond just cognitive defence.

Community-Focused Engagement and Avoiding Securitisation

A key learning from the experiences of efforts to counter terrorism and extremism over the past two decades is the importance of avoiding inadvertently securitising communities. Community securitisation can create fear and mistrust in government, local authorities and security actors by implicitly or explicitly portraying a group as a threat to society or national security. Securitisation thus risks exacerbating discrimination and undermining the human rights of the targeted community; in the worst case, this could even contribute to cases of radicalisation. This also risks undermining trust in government, which is a core objective of hostile actors.

Given this context, it is crucial to determine how to best partner with communities in which a minority may be susceptible to—or even supportive of—hostile states. Lessons can be learned from counter-extremism, which at times engaged with self-appointed 'community leaders', rather than acknowledging the diversity of voices within communities. A reliance on 'moderate imams' in the aftermath of the 9/11 and 7/7 attacks went hand in hand with government approaches to community engagement through unrepresentative gatekeepers, which failed to account for the generational dimension and specific youth dynamics of these threats.

A nuanced assessment is needed to identify potential receptivity to extremism or authoritarianism within specific communities, where hostile states may be able to tap into existing harmful sentiment (for example, antisemitism and anti-Muslim hate). This will also require careful consideration about how likely diaspora communities are to align with or reject hostile state narratives. Diaspora communities should not be treated as inherently receptive to the narratives of their countries of origin. Many members of the Iranian diaspora, for example, have experienced or opposed state persecution and may themselves be targets of transnational repression.

Where sympathies for hostile states may be more likely, it is still important to avoid stigmatisation, or measures that could feed into authoritarian propaganda. For example, Latvia—a key target for Kremlin information operations which has a significant Russian-speaking population—has responded both with innovative preventative public information campaigns and educational initiatives but also withdrawn funding for Russian-language television programming. This risks strengthening Kremlin narratives of discrimination against Russian-speaking minorities. Instead, community-centred programming should be locally rooted, engage transparently with a range of voices, and emphasise social cohesion and human rights.

Other recruitment targets for hybrid operations include groups not defined by a specific identity, but that have other vulnerabilities, such as petty criminals. These individuals may be more vulnerable to recruitment

because of financial hardship, social marginalisation or existing involvement in illicit networks—factors also relevant to terrorist recruitment. Addressing hybrid threats therefore also requires approaches that complement national security measures with social support and crime prevention initiatives, alongside community engagement.

Effectively Learning Lessons from Parallel Fields

One of the lessons from counter-terrorism is that the perceived exceptionalism of this area has at times limited learning from adjacent fields and contributed to siloed policy responses. While hybrid threats involve distinct actors and legal considerations, many of the enabling conditions for this activity will be familiar: grievance, distrust, social fragmentation, opaque financing, online manipulation, criminal recruitment and weak institutional coordination. Any response to hybrid threats should therefore draw deliberately on evidence from established practice, rather than trying to reinvent the wheel.

There are clear opportunities for learning from responses to organised crime, public health, violence and gender-based prevention, strategic communications, and civic resilience. Counter-terrorist financing (CTF) and organised crime are especially relevant because hybrid operations often rely on an underlying infrastructure of proxy organisations, criminal intermediaries, shell companies, opaque funding streams and cyber activism. But such specialist fields have tended to not engage in broader prevention-focused policy discussions.

Similarly, hybrid threats are often coupled with online activity seeking to manipulate on a broader scale, which in turn relies upon social media platform infrastructure (namely amplification), for-hire influencers and PR firms. The reliance on infrastructure in these cases provides ample opportunity for interventions. Alongside the deterrent of criminal punishment, these interventions are typically focused on raising the costs for adversaries to perpetrate such activity and have, to date, involved cross-sectoral coordination.

Recognising the Gender Dimension

On gender and intersectionality, there is an opportunity for policy and practitioner responses to hybrid threats to avoid a major weakness of counter-terrorism and counter-extremism approaches, where opportunities to properly integrate gender and intersectional considerations were often missed or were reduced to narrow and often false assumptions. Women in extremist movements, for example, were often portrayed in mainstream security discourse either as victims, mothers or community gatekeepers, or alternatively vilified as 'unnatural' women and 'bad mothers'. These portrayals have had an impact on policy approaches. Dynamics of gender and other forms of identity also affect recruitment pathways, including through narratives around masculinity, loss of status, humiliation and protection. An intersectional approach is essential because these risks do not operate in isolation. A young migrant woman activist, a queer member of a diaspora community, a racialised journalist, or a religious minority politician may experience hybrid threats differently because multiple aspects of identity shape both vulnerability and visibility. Security policies often do not account for these differences in their design.

Responding to hybrid threats will also require a broader analysis of how hostile actors exploit identity, grievance and divisive social dynamics for recruitment. As has been established by studies on information warfare, misogyny, anti-LGBTQ+ narratives, anti-migrant sentiment, antisemitism, racism and conspiracy theories can all be used as tools for polarisation and democratic disruption. At the same time, diaspora communities, women in public life, journalists, activists and minority groups may be specifically targeted through harassment, intimidation, doxxing or transnational repression efforts. Gender and intersectionality should therefore be treated not as add-ons, but as crucial analytical and response tools for understanding who is targeted, who is recruited, which grievances are mobilised, and which counter-messengers are then afforded credibility with which audiences. Recent research from RUSI highlights how integrating such considerations in threat assessments and interventions can meaningfully enhance strategies to counter state threats.

MAPPING OUT A BROAD SPECTRUM OF POTENTIAL PREVENTION AND INTERVENTION

Recognising the limitations of overly securitised approaches, the 'public health' model of prevention has become increasingly ubiquitous within countering extremism efforts. It draws from wider harm prevention approaches (such as disease mitigation), by seeking to build community and individual resilience through minimising 'risk factors' and boosting 'protective factors'. Such efforts are focused on different 'tiers' of prevention:

- **Primary prevention,** which seeks to foster healthy and resilient communities/individuals.
- **Secondary prevention** focused on interventions for potentially vulnerable individuals.
- **Tertiary prevention** aimed at reaching individuals directly at risk (or engaged in harm).

In this section, we consider how approaching hybrid threats prevention through this lens may have utility in considering how we develop more targeted, proactive and joined-up efforts. The approaches listed below are intended as an initial audit of potentially relevant intervention types from two decades of counter-extremism efforts, rather than a comprehensive account of programming required for preventing hybrid threats.

PRIMARY PREVENTION (BUILDING RESILIENCE)

Upstream interventions are focused on broad-based programming, aimed at building individual and community resilience to harms.

Bolstering social resilience: Social resilience will no doubt be essential to countering hybrid threats. There are various components whose importance we can already grasp—including threat understanding, practical knowledge about dealing with threats, and community efforts to address the fallout from threats. But there is a need to define and build buy-in around what a meaningful whole-of-society approach to resilience looks like, with different roles (e.g. government, researchers, civil society, businesses) clearly articulated. The defining of extremism in vague terms such as 'opposition to British Values' showed the importance of guiding concepts being meaningful and inclusive rather than exclusionary, when thinking about societal resilience efforts. Germany's alternative focus on extremism as 'anti-constitutional activity' may be more instructive in the context of hybrid threats. In the specific context of hybrid threats, there may be potential learnings from the highly promising Baltic and Scandinavian resilience models, while a focus on effective intercommunity dialogue might have particular relevance when considering the importance of engaging diaspora communities in responses.

Cognitive resilience: Inoculation-based strategies for building resilience to extremism and mis/disinformation are gaining traction. There is increasing evidence around the effectiveness of approaches aiming to build up resistance to manipulation by exposing people to (and crucially providing them the skills to deconstruct) diluted forms of harm. Research by the German Federal Crime Agency has also demonstrated the potential of offering positive alternative narratives to reduce the appeal of extremist ideologies, rather than attempting to deconstruct propagandists' narratives. Parallel efforts to raise awareness around harms (such as hostile actor recruitment), should learn lessons around the specific role of government and media, including in incident response for post-crisis event contexts.

Education efforts: Education in digital citizenship plays a crucial role in developing media and information literacy, advancing critical thinking and building resilience among younger audiences against online manipulation. There are lessons to be learned from the implementation of more targeted counter-extremism programming such as the UK's statutory Prevent Duty in schools, including the potential risk of securitising classrooms. Lessons and best practice approaches will also need to be drawn from partner countries who have been on the frontlines of hybrid warfare. For example, the Baltic states have trialled a series of successful interventions, expanding preventative public information campaigns and public awareness efforts to counter hostile information operations, including by integrating pre-bunking and debunking resources into school curricula.

There are also important lessons to be drawn around school-based programming engaging education stakeholders beyond teachers—e.g. councillors, safeguarding leads and parents—as well as more informal education settings, such as youth clubs. While the profile of hybrid threat targeting appears to be younger (in particular impacting teenagers), one lesson from counter-extremism is the importance of educational interventions not stopping with young people but also including adults, as the impacts of online harms cut across different generations in distinct ways.

SECONDARY PREVENTION (TARGETED EFFORTS TO ADDRESS VULNERABILITIES)

Targeted strategic communications efforts: Spanning both primary and secondary prevention, strategic communications efforts (including the promotion of counter or alternative narratives) have been a central pillar in deterring audiences from gravitating toward extremist ideologies, movements or groups. The strategic communications toolbox encompasses everything from traditional advertising and online campaigns, television and radio series, to diplomatic efforts and policies, and one-to-one engagement. So far, while national governments and multilateral institutions have become more aware and more vocal about hybrid threats, they still lack a coherent public communications strategy to push back against authoritarian state propaganda.

Hybrid threat actors have proven effective at deploying various communication tools to garner support or influence audiences. Learning from counter-extremism, strategic communications efforts to address hybrid threats are likely to benefit from being rooted in an evidence-driven understanding of target communities based on insights from within. Any communications efforts operating from preconceived conceptions of communities will likely fail to degrade the appeal of recruitment. Designing a comprehensive strategic communications approach requires evidence-based research, international, national, and local networks of support, and access to the means to deliver messaging both at a hyper-localized level and international scale. It also requires coherence between message and action, which is why it often fails when strategic communications efforts only focus on the message, while wider actions are in contradiction or undermine it.

Alternative narratives have been championed as a way to indirectly undermine extremist messaging by focusing on commonly faced vulnerabilities and grievances weaponised by extremists, such as loneliness, aggression, impulsive behaviour, or a lack of confidence. Since alternative narrative campaigns often focus on a wider set of issues compared to counter narratives—and sometimes a broader audience—they may be better suited to mass media, or larger campaigns. Such campaigns benefit from contextualized local knowledge, voices and organizations that can deliver an alternative message with meaningful resonance for audiences. While the broader appeal of these messages will likely find more of an audience, it will inevitably be very difficult to measure if an alternative narrative decreases or stymies a specific extremist group or narrative.

For hybrid threats, where there is often a nexus to criminality, strategic communications approaches will likely require both police and traditional anti-crime messaging and programmes, along with specific terrorist and extremist counter narrative programmes. Informational approaches will likely be ineffective in countering recruitment for hybrid operations which are leveraging local criminal networks: in these cases, the underlying incentives will often be economic rather than being driven by grievances, narratives or information that could be debunked or fact checked. Targeted messaging efforts seeking to address any relevant ideological dimension (outlined in greater detail below) might be designed to complement existing broader campaigns focusing on crime prevention and violence reduction.

Direct interventions and referral to support services: 'Redirection' approaches have emerged as a popular methodology for online interventions to counter extremism, based on flagging individuals engaging in risky online behaviour and diverting them to positive alternatives. In considering whether such efforts may have efficacy in responding to the hybrid threat landscape, we need a more in-depth understanding of how people are engaging in online spaces specific to hybrid threats, as well as how individuals are being directed towards harmful networks. There are likely learnings from broader crime prevention research in considering what mechanisms might provide the most appropriate support services (counselling, psycho-social support, mentorship) for hybrid threats, if indeed this is relevant at all given, given the financial nature of much of this recruitment.

TERTIARY PREVENTION (MINIMISING ACUTE HARM AND MANAGING IMPACTS)

Disruption: Alongside blunting the impact of adversarial tactics, effectively raising the cost of attack is a crucial part of many governments' prevention and deterrence playbook. More muscular counter-extremism efforts have increasingly focused on the disruption of harmful actors—including those below the threshold of terrorism who nonetheless create conditions for serious harm. In the hybrid threats domain, there is a need to consider strategies aimed at creating additional friction for the activities of harmful networks, rather than operating from a largely defensive posture. Such efforts are likely to require important considerations around governments' risk appetite around proactive measures, including deploying offensive information operation and cyber capabilities, and the use of asymmetric tactics as part of an actionable plan for deterrence.

Counter-financing dimension: Monetisation is a crucial but often overlooked part of the playbook to curb harmful activity. Highly effective provisions have been developed over the past two decades in the fields of CTF, as well as through state actor-focused sanctions regimes. Given the centrality of crypto and digital payments to the hybrid threat landscape, there are clear lessons to be learned from CTF about how regulations, frameworks and mechanisms can close loopholes being exploited by bad actors. However, a key lesson from efforts to mitigate terrorist financing is the importance of carefully considering potential trickle-down consequences of such blunt methods, as seen in examples of the debanking of individuals and financial sanctions against civil society groups with specious linkages to terrorism.

Efforts to counter malign finance and undesirable foreign funding can draw important lessons from attempts to address foreign political funding. Earlier this year the UK's Rycroft Review highlighted that safeguarding democratic processes requires greater transparency over the ultimate source of funds and greater powers for authorities to investigate potentially hostile financial activity. The Review also prompted an immediate ban on cryptocurrency donations in March 2026 pending stronger regulation. There are approaches used within cybersecurity that could be instructive, including blockchain analytics and network mapping, as well as enhanced information-sharing between government and industry (via the Information Sharing and Analysis Centre - ISAC - model). Such approaches could similarly be used to identify the suspicious crypto transactions that are often associated with hybrid attacks, for example in the case of Roman Lavrynovych, who was seemingly paid to carry out arson attacks targeting properties linked to then Prime Minister Keir Starmer.

Disengagement and deradicalisation: 'Deradicalisation' is likely a less useful frame than disengagement when considering more opportunistic and less ideologically motivated hybrid threats, when compared to extremist radicalisation. However, there are still important considerations around the potential 'ideological' element of rejecting liberal democratic systems, and its implications for attitudinal interventions. One UK judge described the 2024 arson attack carried out by a 21-year old British drug dealer linked to Russian intelligence and the Wagner Group as an example of "young men who were prepared to undergo a form of radicalisation and betray their country for what seemed easy money". One of the broader lessons from two decades of CT and P/CVE work was the considerable challenge associated with 'talking people off the ledge', compared to the relative dividends of investing in upstream values-based work. It will be crucial to better quantify the relative potential and trade-offs between different types of interventions approaches going forward.

Law enforcement and security services action: Consistent and proportionate enforcement against illegal activity is crucial for effective deterrence of hybrid threats. The UK's new National Security (State Threats) Act has established a new framework equivalent to terror designations designed for foreign state-backed groups to designate the Islamic Movement of the Companions of the Right and the GRU Volunteer Corps (the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation Volunteer Corps), making it illegal to express support and mandating social media platforms to mitigate risks related to these groups' content. Meanwhile, the European Union's designation of the IRGC as a terrorist organisation, shows the potential of creatively using existing legislative tools to prosecute hybrid threats effectively, even if the banning of groups cannot address violent threats that have no affiliation to formal groups. Beyond ensuring consistent application of legislation, lessons from counter-extremism show the particular importance of law enforcement training focused on human rights and civilian protection laws/norms, given the profound community impacts of hostile state activity.

CONCLUSION & RECOMMENDATIONS

This paper aims to outline high-level lessons from two decades of efforts to counter violent extremism and inform prevention efforts to mitigate the growing hybrid security threat faced by European democracies. This lines up closely with the notion of "democratic defence" put forward by Protection Approaches, with another recent report by Dame Sara Khan and Matthew Godwin highlighting that democratic distrust, social fragmentation and the mainstreaming of extremist narratives are closely interconnected. As part of their conclusions, they argue that policies to strengthen resilience against hostile state activity and domestic extremism should be integrated rather than treated as distinct policy tracks.

Our paper suggests that rather than unnecessarily reinventing the wheel, key learnings can be drawn from the established policy area of counter-extremism. This includes the need to ensure effective whole-of-government policy responses, as well as building durable systems for national-local government cooperation. Learning from counter-terrorism, it is crucial to embed digital policy dimensions into responses from the outset, given the centrality of online platforms across the entire lifecycle of hybrid threats—from propaganda production and dissemination mechanisms to audience consumption of harmful online content. And it is crucial to learn from the challenges of potential over-securitisation hampering meaningful community engagement, as well as the importance of widening narrow violence prevention approaches in how we construct preventative approaches.

Drawing on a 'public health model' of prevention, the paper considers a range of tried and tested interventions aimed at boosting protective factors and mitigating risks and vulnerabilities, which might be relevant to countering hybrid threats. Potentially transferable approaches range from more upstream 'inoculation' against authoritarian propaganda through education and digital literacy programming, to more targeted strategic communications efforts aimed at reaching at-risk communities. Meanwhile at the 'sharper tip', lessons from counter-extremism disengagement and deradicalisation, counter-financing and network disruption efforts may have applicability to these emerging challenges. Learning from challenges in evaluating extremism prevention efforts, deep research is required on what works for interventions geared towards the specificities of hybrid threats, rather than merely 'copying and pasting' existing approaches.

This paper is intended to provide an initial set of considerations for designing strategic cross-government responses to the tech-facilitated hybrid warfare being waged against European democracies, drawing on key lessons from adjacent policy areas such as counter-terrorism. Further deep dives will be crucial for establishing more granular considerations around specific prevention domains, from fostering societal resilience to bolstering strategic communications and enforcing digital regulation. Meanwhile, there is a clear need for a coordinated research agenda that seeks to address gaps in both our understanding of the evolving threat, as well as what works from an intervention perspective. Here, new coalitions and partnerships will be essential for advancing this urgent policy conversation across the often-siloed domains of national security, foreign policy, public safety and societal resilience, bringing together important complementary lessons from across the policy, practitioner and research communities.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Toronto | Washington DC

www.isdglobal.org