The US National Strategy on Countering Domestic Terrorism as a model for the EU

Eviane Leidig and Charlie van Mieghem
The US National Strategy on Countering Domestic Terrorism as a model for the EU

Eviane Leidig and Charlie van Mieghem
Policy Brief
September 2021
About ICCT

The International Centre for Counter-Terrorism – The Hague (ICCT) is an independent think and do tank providing multidisciplinary policy advice and practical, solution-oriented implementation support on prevention and the rule of law, two vital pillars of effective counter-terrorism.

ICCT’s work focuses on themes at the intersection of countering violent extremism and criminal justice sector responses, as well as human rights-related aspects of counter-terrorism. The major project areas concern countering violent extremism, rule of law, foreign fighters, country and regional analysis, rehabilitation, civil society engagement and victims’ voices.

Functioning as a nucleus within the international counter-terrorism network, ICCT connects experts, policymakers, civil society actors and practitioners from different fields by providing a platform for productive collaboration, practical analysis, and exchange of experiences and expertise, with the ultimate aim of identifying innovative and comprehensive approaches to preventing and countering terrorism.

Licensing and Distribution

ICCT publications are published in open access format and distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License, which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About ICCT</td>
<td>iii</td>
</tr>
<tr>
<td>Abstract</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Conceptual Overview</td>
<td>3</td>
</tr>
<tr>
<td>Counter-Terrorism Framework</td>
<td>4</td>
</tr>
<tr>
<td>Information gathering</td>
<td>4</td>
</tr>
<tr>
<td>Prevention</td>
<td>6</td>
</tr>
<tr>
<td>Enforcement</td>
<td>8</td>
</tr>
<tr>
<td>Building resilience</td>
<td>9</td>
</tr>
<tr>
<td>Policy Recommendations</td>
<td>10</td>
</tr>
<tr>
<td>Bibliography</td>
<td>14</td>
</tr>
<tr>
<td>About the Authors</td>
<td>17</td>
</tr>
<tr>
<td>Eviane Leidig</td>
<td>17</td>
</tr>
<tr>
<td>Charlie van Mieghem</td>
<td>17</td>
</tr>
</tbody>
</table>
Abstract

The United States National Strategy for Countering Domestic Terrorism is built on a comprehensive threat assessment of domestic terrorism as ordered by President Biden, and prioritises far-right extremism. Although the conceptualisation contains certain flaws, the strategy acknowledges this rising threat in a comprehensive and evidence-based assessment. In this Policy Brief, we highlight the US Strategy as a blueprint for improving the EU counter-terrorism model and identify four shared areas in these frameworks: 1) Information gathering, 2) Prevention, 3) Enforcement, and 4) Building resilience. We recommend that the US and EU could mutually learn from one another’s approaches on issues such as multi-agency cooperation, regulation of technology companies, and countering dis/misinformation. Both the US and the EU counter-terrorism agendas should furthermore apply a gender lens throughout their respective strategies in order to ensure more nuanced and accurate programming.

**Keywords:** US, EU, counter-terrorism, far-right extremism
Introduction

In December 2020, the European Commission established an EU counter-terrorism agenda. The goal of the agenda is to build on existing policies within the different EU institutions and Member States to improve the broader framework to counter current and emerging threats and speed up the impact of measures on the ground. This agenda is based on four pillars: anticipate, prevent, protect, and respond.

Interestingly, there is little specific mention and addressing of the far-right threat in this agenda. The same applies to other EU counter-terrorism documents, such as the EU Security Union Strategy 2020-2025. This is unexpected, taking into consideration recent far-right attacks, such as the terrorist attack in Hanau, Germany, and anti-COVID-19 and anti-Black Lives Matter protests that occurred in 2020 in different European Union Member States.

This also stands in stark contrast to the June 2021 release of the United States National Strategy for Countering Domestic Terrorism. This document specifically addresses domestic terrorism, focusing on the far-right, as a historic and developing threat that needs to be addressed, while safeguarding the civil liberties and rights of the American people. The strategy is innovative for being the first US counter-terrorism strategy that specifically focuses on domestic terrorism, albeit present with its own limitations, as discussed below. Importantly, the US Strategy was formulated as a direct response to the January 6, 2021 insurrection at the Capitol and attempts to delegitimize the election of President Biden. This defining moment in US history would pave the way for the emergence of a national strategy on domestic terrorism. The issue of domestic terrorism became a priority for the new Biden administration from the beginning, as winter/spring 2021 witnessed an all-hands-on-deck approach by officials in intelligence, law enforcement, homeland security, and defence, leading up to the publication of the US Strategy.

The US and EU counter-terrorism models can also be situated in relation to the recent UN Global Counter-Terrorism Strategy’s seventh review, which explicitly identifies terrorism and violent extremism to include “on the basis of xenophobia, racism and other forms of intolerance” in addition to religion. Although not labelling it far-right extremism per se, this aligns with our proposed conceptual definition below and reflects a broader global response to tackle far-right extremism as a current and emerging threat.

3 European Commission, “EU Security Union Strategy: connecting the dots in a new security ecosystem”, July 2020, https://ec.europa.eu/newsroom/content/eu-strategie-f%C3%BCr-die-sicherheitsunion-zusammenf%C3%BCrchrung-der-einzelma%C3%9Fnahmen-einem-neuen_en
This Policy Brief highlights the ways in which the US Strategy can serve as a blueprint for a similar EU counter-terrorism agenda that focuses specifically on the increasing threat of far-right extremism, while simultaneously suggesting opportunities for an improved approach for the US from an EU perspective. Providing recommendations at a comparative level will help advance global efforts to counter the growing far-right extremist threat that is becoming increasingly international in scope.

**Conceptual Overview**

We employ the concept of ‘far-right extremism’ in this Policy Brief in which *far-right* refers to ideational principles (i.e. nationalism combined with xenophobia, ethnicity as a determinant of belonging to the national community, and an authoritarian stance towards law and order), and *extremism* refers to behavioural principles (i.e. engaging in or in support of anti-democratic and violent methods). We use this working definition as a basis of comparison for the US and EU counter-terrorism strategies since each operates according to separate terminology. It should be noted that the definition we use in this Policy Brief is much narrower than the US and the EU strategies, but adheres to the largely agreed-upon definition with the scholarship on the far-right.8 Below, we address some of the definitional challenges proposed by the US Strategy. Given that the EU counter-terrorism model does not explicitly identify the far-right as a threat, we discuss below the US Strategy as a blueprint for conceptualising far-right extremism.

The Biden administration’s National Strategy for Countering Domestic Terrorism (herein the US Strategy) refers to REMVE as constituting a dominant threat in domestic terrorism—and is the focus of this Policy Brief. REMVE is “racially or ethnically motivated violent extremists and networks whose racial, ethnic, or religious hatreds lead them towards violence, as well as those whom they encourage to take violent action”.9 Building off the previous administration’s introduction of the concept of REMVE, this threat category is the most ideologically similar to the far-right as it distinguishes between ‘in-group’ and ‘out-group’ according to racial, religious, and sexual determinants. The REMVE definition, however, is problematic in that it focuses primarily on actors who engage in violence, which does not adequately capture the spectrum of far-right activity that poses a threat to civil society.

---

Counter-Terrorism Framework

In this Policy Brief, we highlight the similarities and differences between the US and EU counter-terrorism models. Our assessment of the threat landscape for both CT models follows the same framework: 1) Information gathering, 2) Prevention, 3) Enforcement, and 4) Building resilience. By comparing these approaches, we aim to highlight best practices and policies in governance strategies towards countering far-right extremism.

Information gathering

The first pillar of the EU counter-terrorism agenda aims to better anticipate emerging threats. It outlines the available instruments to do so, such as risk assessments on air and train travel, and ongoing infrastructural mechanisms to improve anticipation. It also aims to identify areas in which anticipation itself can still improve, such as better use of strategic intelligence, an extension of the application of risk assessment, and ways to integrate foresight in the policy cycle. In this way, security research combined with enlarged investments in new technologies can contribute to better EU anticipation of a terrorist threat.

Comparatively, the first pillar of the US Strategy, “Understand and share domestic terrorism-related information”, is more comprehensive in scope. In addition to increased cooperation between multi-agency (security) stakeholders at various levels of government, there is an explicitly research-driven approach to identify and share resources that cover “relevant iconography, symbology, and phraseology” used by violent extremists and terrorists. This is an innovative approach that mitigates risk beyond public security and infrastructure. Stakeholders that are equipped with the necessary tools to identify propaganda and drivers of mobilisation allows for effective anticipation efforts at an early stage. Focusing interventions on the everyday places and spaces of far-right community building, often online, means identifying the discourse and images that circulate within these interactions that could escalate to violence. Thus, the US counter-terrorism approach emphasises online spaces that serve to communicate, recruit, and mobilise, sometimes drawing upon ideological inspiration from abroad (either influenced by or in direct contact).

The US Strategy makes a welcome effort towards recognising the transnational connections of domestic violent extremists, and in particular the REMVE dimension as a nexus for international concern. REMVE actors based in the US have strong transnational ties to REMVE actors abroad in pursuit of similar goals. It recommends that the Department of State assess and designate foreign entities linked to domestic terrorism as “Foreign Terrorist Organizations or Specially Designated Global Terrorists”, which is a major advancement. With the exception of one organisation (Russian Imperial Movement), there is currently no far-right organisation on this list, which leans heavily towards jihadist groups and individuals. By designating far-right

---

16 ibid., 17-18.
groups as Foreign Terrorist Organisations, the list provides legitimacy and impetus for state and supranational actors to implement necessary security measures to respond to these organisations appropriately. Unfortunately, the designation is complicated given current legal restrictions that prohibit the US government from designating domestic terrorist organisations which are not foreign entities, i.e., operate abroad. The result is that prevalent far-right extremist organisations that operate in the US are not accounted for due to current restrictive frameworks. A related challenge is that the contemporary far-right extremist threat is more likely to transpire from ‘lone wolf’ attackers than organized group activity.

Another problematic aspect of the US Strategy is a false dichotomy between domestic and foreign terrorism. Here, domestic terrorism equates to a far-right threat, and foreign terrorism signals an Islamist threat (as evident by the list of Foreign Terrorist Organisations). Yet, domestic terrorism can be an Islamist threat and foreign terrorism a far-right threat. Although Islamist extremists may be inspired by foreign entities, the rise in far-right lone actor attacks represents a similar international phenomenon. This can be traced through the legacy of the 2011 attacks in Norway upon subsequent domino effect incidents such as the 2019 attacks in Christchurch, Poway, and El Paso, in which each perpetrator was inspired by the previous (foreign) attacker.

Similarly, perpetrators of Islamist terrorism are often citizens of, and born into, Western countries. Such examples include the two brothers behind the Charlie Hebdo shooting in 2015, and one of the perpetrators of the San Bernardino, California attack later that year. Although the Charlie Hebdo perpetrators identified as belonging to al-Qaeda, the couple behind the San Bernardino shooting were labelled as “homegrown violent extremists” who sought inspiration from Islamist ideology but remained unaffiliated to any group. The foreign-domestic terrorism dichotomy is therefore questionable. Further, labelling Islamist terrorism as ‘foreign’ might have negative effects: it can reinforce the stigmatisation and securitisation of suspect communities, such as questioning claims to citizenship.

The final transnational element of information sharing pertains to a renewed focus on financing, including foreign transactions. Building upon previous measures to track Islamist financing could be an effective strategy to determine the scope and scale of far-right financial activity. The European Commission already has an anti-money laundering Directive in place to prevent the abuse of financial systems, including online currencies and other emerging financial systems for terrorist (financing) purposes. Included in this directive is the Commission’s mandate to identify high-risk third countries to address in the financial policy.

17 At the same time, we warn of an overreliance on these lists given that the contemporary far-right threat is often not structured according to traditional organizations, but rather through networks and groupuscules (see Pietro Castelli Gattinara and Andrea L.P. Pirro, “The far right as social movement,” European Societies 21, No. 4 (April 2018): 447-462).
We acknowledge that in information sharing efforts, as well as the pillars discussed below, the US and EU have very different governance structures and legal constraints that guide these approaches. In particular, the US is heavily reliant on state and local authorities who share resources with federal officials but are under no obligation to adhere to the US Strategy. This level of localisation differs from the EU’s relationship to its Member States who create national mandates in line with a regional framework.

Prevention

The second pillar of the EU counter-terrorism model aims to prevent terrorist attacks by addressing the early stages of the problem, particularly connected to the radicalisation phase. Focal points within the EU strategy in this area are promoting inclusion through education and social work, preventing radicalisation in prisons, improving reintegration of former detainees into society, and the handling of returning foreign terrorist fighters and their families into society. These actions are tailored to the Islamist threat that characterised responses in the previous counter-terrorism strategies.

Within the goals presented in the EU counter-terrorism agenda, especially the dissemination of online extremist content and the promotion of inclusion, there is more capacity to address the far-right threat. An important caveat in this pillar is the absence of an explicit far-right tailored approach, which heightens the risk of overlooking or underestimating the dangers posed.

On the contrary, the US Strategy explicitly focuses on the far-right. The second pillar, “Prevent domestic terrorism recruitment and mobilization to violence”, aims to bolster resilience while reducing the widespread availability of recruitment materials online. It builds on a “public health-focused violence prevention” approach. While this is unclearly phrased, it refers to a data-driven approach to analyse indicators of violence. This method stems from avoiding critiques in the past that prevention efforts were not sufficiently data-driven (thus resulting in the stigmatisation of groups and individuals), and the necessity to shift to expert assessments of indicators of mobilisation. In particular, this will be manifested in “a new edition of the Federal Government’s Mobilization Indicators booklet that will include for the first time potential indicators of domestic terrorism-related mobilization”, whereas previous editions have focused on international terrorist groups and individuals. This resource will be useful, but given that previous editions of the booklet have focused on group-oriented mobilisation indicators, the threat of far-right terrorism is more diffuse and thus resource allocation will need to reflect these operational realities. Further, enacting a data-driven approach should weigh heavily on human rights concerns so as to avoid undue surveillance and privacy violation, whilst upholding free expression.

This “public health-focused” prevention approach is, however, confusing to interpret. Without context, it can easily be understood as a comprehensive approach comprising of social and medical services, not least including interventions from parents, educators, mental health professionals, and social workers. Indeed, experts on far-right extremism have described the phenomenon as a “public health problem”, arguing that combating extremism needs to be redirected through training and resources at the local level to build community resilience against radicalisation.25

23 According to an official who spoke at a Washington Institute for Near East Policy CVE roundtable under Chatham House Rule.
As a mechanism to further strengthen resilience, the US Strategy promotes “enhancing media literacy and critical thinking skills”.26 The aim is to strengthen resilience to dis/misinformation, and “cultivate digital literacy and related programs, including educational materials and interactive online resources such as skills-enhancing online games”.27

Relatedly, the US Strategy also provides an official endorsement of the Christchurch Call. This initiative was launched by the governments of New Zealand and France in response to the 2019 Christchurch attack, demonstrating a joint commitment by governments and tech companies, to “eliminate terrorist and violent extremist content online”.28 This official endorsement by the Biden administration is a significant step, and echoes the UN Global Counter-Terrorism Strategy’s recognition of the Christchurch Call,29 although the US has long maintained a representative in the Global Internet Forum to Counter-Terrorism (GIFCT),30 an initiative between tech companies, governments, and civil society organisations to counteract terrorist use of technology. There are, however, more concrete steps that the US can take in countering far-right extremism online, borrowing from the EU approach.

The EU Strategy is better equipped when it comes to online regulation pertaining to terrorist and violent extremist content. Within the “Prevent” pillar, the EU focuses upon a number of initiatives to counter extremist ideologies online. Regulations prioritise content rather than actor types,31 which reflects the reality of the far-right threat as diffuse and fragmented. In order to implement the removal of such content, the EU has introduced the Digital Services Act, which requires tech platforms to evaluate their obligations and assess risks posed to users and society at large. In April 2021, the European Parliament adopted regulation 2021/784 on addressing the dissemination of terrorist content online. The regulation forces hosting service providers to remove any flagged content within one hour after receiving an order from a competent authority. Further handling of the breach of this law, such as fines or other sanctions, remains the responsibility of the Member States.32 The new regulation, however, has been criticised by human rights agencies for its broad definition of terrorist content.33

Driving this response is the EU Internet Forum (EUIF), which develops guidance on extremist materials available online. During the sixth Ministerial Meeting in January 2021, the need for increased collaboration and guidelines in curbing violent far-right content online was raised.34 The EUIF also hosts the EU Crisis Response Protocol: “a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of terrorist and violent extremist content online”.35 These initiatives extend to international partners such as GIFCT and the Christchurch Call. The EU strategy has taken steps to expand efforts towards countering hate speech online in addition to terrorist and violent extremist content. Through the EU Code of Conduct, technology companies voluntarily pledge to take action on illegal hate speech on the

27 ibid., 22.
30 Global Internet Forum for Counter-Terrorism, “Governance,” https://gifct.org/governance/#government
31 European Union, A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, p. 6.
33 Nery Ramati, “The Legal Response of Western Democracies to Online Terrorism and Extremism”, 2020, p. 89.
basis of race, ethnicity, religion, gender, or sexuality. The EU has taken bold steps to recognise the connection between terrorism and violent extremism and hate speech, as related categories constituting a spectrum of online activity.

At the same time, we caution of the impact of online governance on human rights and freedom of expression. Countries utilise “four commonly seen legal techniques that are used to limit extremist content: the blocking and removal of online content; the surveillance of online activity; the criminalising of certain online public expressions; and the use of online content as a justification for applying restrictive administrative measures”. These repressive tools must be assessed in line with potential overreach on privacy and freedom of speech.

The Radicalisation Awareness Network (RAN) is also an important EU initiative to address extremism in prevention efforts. RAN is increasingly researching far-right extremism and has held workshops and training sessions to address related problems for EU Member States in the form of project-based collaborations. However, these trainings and consultations have so far been voluntary for the Member States, and are not part of a coherent EU counter-terrorism policy and practice framework on far-right extremism.

Finally, the US Strategy takes a timely and necessary approach in prevention by highlighting the role of the Department of Defense in training current and retired military personnel on identifying recruitment tactics of violent extremists. Veterans will also be able to report such recruitment measures through appropriate mechanisms. Although in an EU context this will most likely fall under Member State domestic sovereignty and jurisdiction, the EU can make recommendations to individual states.

Enforcement

The overarching goal of the third EU pillar, “Protect”, is to avoid or minimise the harm of terrorist plots, should prevention fail. This entails the protection of borders, public places and infrastructure, as well as adequate prosecution to safeguard EU citizens. An important element is the use of EU intelligence and technologies to protect Member States from threats that enter or move within the borders of the EU, with a strong focus on external threats. To control the security of EU borders, the Schengen system works as a basic framework, with support from Frontex and eu-Lisa to optimise protection in this field. However, controlling external borders focuses predominantly on Islamist terrorism, and the threat that foreign terrorist fighters pose to the EU. The focus on external threats is not translated to protection from the increasing internationalisation of far-right movements. New, appropriate responses to emerging threats should always be adapted and created. In the case of combating the far-right threat, digital judicial cooperation is a major challenge, although Eurojust has recently commissioned expert workshops on violent right-wing extremism and terrorism.

36 Ramati, “The Legal Response of Western Democracies to Online Terrorism and Extremism”, p. 7.
40 EU LISA, “Who we are,” eulisa.europa.eu/About-Us/Who-We-Are
The EU aims to reach more efficient mechanisms for cross-border access to e-evidence. Further, challenges to criminalising terrorist offences lie in listing certain groups and networks as terrorist organisations.

Similarly, pillar three of the US Strategy, “Disrupt and deter domestic terrorism activity”, focuses upon the prosecution of crimes and the rule of law as a multi-agency response. In addition, potential legislative reforms to bolster national security must be protected from abuse of overreach, a consequence of the lessons learned from the War on Terror. However, protection of free speech embedded in the First Amendment of the US Constitution provides a distinct foundational legal structure that differs from the EU, as criminal prosecution remains a challenge to convict individuals for conduct that falls short of physical violence. Finally, the US Strategy takes a bold step in improving the screening and vetting process for military, Federal law enforcement, and government employees with a security clearance to ensure that such individuals do not hold ties to domestic terrorism. This extends to the Department of Defense, tasked with “reviewing and updating its definition of prohibited extremist activities among uniformed military personnel” and policy recommendations for civilian employees and contractors.

**Building resilience**

The fourth pillar in the EU counter-terrorism agenda, “Respond”, focuses on areas to improve or optimise during and after a terrorist attack. One of the areas addressed in this pillar focuses on the role of Europol in sharing and coordinating intelligence. In the aftermath of a terrorist attack, authorities and the media have a duty to inform the public with relevant and useful information. The tackling of dis/misinformation, as a vector towards polarisation, is specifically included in the US Strategy for this reason. For similar purposes, the EU strategy also emphasises victim support to address grievances and prevent radicalisation, counter-reactions, or future retaliatory attacks. This tailored support for victims builds upon the EU’s Victims’ Rights Directive, which establishes minimum standards on the rights, protection, and support of victims of crimes, and access to justice. This reflects an international effort to recognise the role of victims of terrorism in promoting global solidarity and ensuring justice.

These future-oriented solutions to building resilience are reflected in the fourth pillar of the US Strategy as, “Confront long-term contributors to domestic terrorism”. While some elements are unique to the American context compared to the EU, i.e. gun violence, most other aspects are applicable elsewhere. Tackling racism, early intervention and care for those at risk, and civic education to promote tolerance and respect for diversity are social factors that can also be implemented in an EU approach. An additional focus on building economic security and sustainable development is likewise relevant, however, we caution against drawing a causal relationship between those in poor employment conditions and opportunities for involvement in far-right extremism. Current research reveals that supporters of the far-right are not exclusively economically marginalised, but that economic grievances should be understood in combination with cultural anxieties.
Rather, parallels between sustainable economic development and extremism should focus upon the potential of perceived loss within narratives of recruitment and radicalisation used by extremists.

Finally, the US Strategy directly addresses growing public distrust in government and extreme polarisation, framed as fuelled through dis/misinformation on social media platforms. Preventing further polarisation and anti-establishment or anti-government sentiments is likewise essential within the EU, primarily since the existence and legitimacy of the EU depends on public trust. Increasing anti-EU sentiments are on the rise, especially among the far-right. These groups and individuals blame the EU for economic and migration problems, which is escalated through online discourse and interactions. While social media mechanisms are pertinent in fostering societal discord, they ultimately amplify and reproduce pre-existing social and cultural grievances. Extremists exploit these divisions to further their own goals.

Policy Recommendations

The recently published US National Strategy for Countering Domestic Terrorism is a first-of-its-kind policy document in specifically addressing far-right extremism. Despite certain flaws in conceptualisation, it acknowledges this rising threat. The analysis above shows that the EU can draw lessons from the comprehensive US approach in anticipating and preventing far-right terrorism, as well as in protecting and building resilience within society; we have, however, identified areas from EU policy that could benefit the US Strategy. In conclusion, we recommend the following policy interventions to improve both the US and EU counter-terrorism models.

The recommendations put forward are structured according to the framework above, tailored to specific concerns regarding information sharing, prevention efforts, enforcement, and building resilience. However, two general recommendations withstand overall:

- Firstly, the EU counter-terrorism strategy should explicitly include far-right extremism as a current and emerging threat in its framework. While Islamist terrorism should continue to remain on the counter-terrorism agenda, the EU is behind on recognising and developing measures to specifically challenge the rise of the far-right. Individual Member State efforts need to be consolidated into a comprehensive, regional framework.

Despite this recent emphasis on far-right extremism, we caution against employing a false dichotomy between domestic and foreign terrorism given the contemporary transnational character of the far-right. Instead, we recommend that concepts based on ideology (i.e. far-right, Islamist) are more analytically useful, and can have consequent practical implications for interventions. Assessing threats based on motive rather than national borders can potentially foster better allocation of resources and inter-agency cooperation, including foreign allies, to counter these emerging transnational threats.

The second general recommendation, which applies to both the US and EU counter-terrorism strategies, is a distinct focus on gender dimensions, which is currently lacking. While the US strategy does acknowledge that women and girls, as well as LGBTQI+ individuals, might be the victims of far-right violence, or the threat of single-issue ideologies such as incels and “gender-motivated violence” in domestic terrorism, a gender lens should be thoroughly incorporated into both frameworks. This spans from understanding the threat through the gendered narratives used to recruit and mobilise individuals; to tailoring prevention efforts around gender roles; enacting prosecution measures based on drivers of men’s and women’s participation in violence and crimes, and building long-term solutions that recognise gender as an intersectional identity in combating far-right extremism. Both the US and EU strategies would benefit from the inclusion of the UN Global Counter-Terrorism Strategy’s explicit recognition of integrating gender dynamics in counter-terrorism programming and its impact, as well as the Special Rapporteur’s identification of the gendered effects of counter-terrorism.

Regarding the first pillar, information sharing:

- We recommend that the US develop a similar approach to the EU counter-terrorism strategy by combining perspectives from multi-agency government stakeholders and civil society actors dedicated to evidence-based research that can inform anticipation efforts. In particular, academics, researchers, and community organisations could offer expertise on current and emerging threats, including online, signalling new trends and areas of potential risk that could face oversight by state actors—a type of “whole-of-society approach” described by the UN Global Counter-Terrorism Strategy. The EU invests in Horizon Europe, a key funding programme for research and innovation, which serves as a valuable resource for the security policy cycle. A similar scheme would benefit the US strategy through a long-term, sustainable partnership between government agencies and the research community, to help create a common understanding of the threat landscape of far-right extremism.

- We recommend that the US improves its designation of far-right organisations to include prevalent entities, but caution against solely depending on this mechanism to understand the contemporary threat. Similarly, we recommend that the EU improves designation measures given that the current terrorist list barely includes any far-right extremist persons and entities. As of now, EU Member States maintain their own individual lists that include
far-right extremists. These individual State lists should be incorporated into an overall EU strategy. The current EU approach to understanding transnational elements and delivering responses is Islamist-focused, risking oversight for the increasing transnationality of the far-right. The Radicalisation Awareness Network (RAN) has commissioned research to address this gap, but no consequent policies targeting transnational far-right extremism have been adopted in the EU counter-terrorism strategy thus far. The far-right is not a threat that can be addressed by states on a merely national level — its transnational nature highlights the need for a wider EU strategy, supportive of individual Member States’ policies. However, it should be taken into account that the nature and structure of far-right terrorists differ from Islamist terrorists. Far-right terrorism is often individually-driven and lacking membership in an organisation. Various methods should be explored to incorporate the far-right threat on such lists.

- In terms of financing, while some of the third countries identified by the EU as high-risk are based on the existing terrorist watch list, and should remain, the country list should be revised in order to adapt to transnational flows of far-right financial activity. We further recommend that in addition to traditional currency flows, digital currency such as cryptocurrency should be explicitly incorporated in this approach. Far-right extremists increasingly rely on cryptocurrency funding streams to build support.

For the second pillar, prevention:

- We recommend that the US Strategy would benefit by fully and explicitly incorporating other aspects of public health interventions ranging from individual factors (psychological and behavioural) to societal factors (gender and racial determinants, economic circumstances, and environmental influence) in describing its “public health” approach. The EU’s strategy of supporting local civil society actors in prevention efforts, particularly through the inclusion of educators, youth and social workers, and community organisations at the grassroots level, in designing proactive interventions at an early stage to prevent radicalisation has translatable potential.

- We emphasise that the US Strategy could benefit from the EU approach concerning online regulation and coordination with tech companies, as manifested through efforts of the EU Internet Forum. On the other hand, adopting a similar model to the US on promoting digital and media literacy skills within the EU to prevent far-right extremist radicalisation, while also targeting social polarisation through educational initiatives, is an advantage. While the EU

58 Annelies Pauwels, “Contemporary manifestations of violent right-wing extremism in the EU: An overview of P/
sites/default/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/ran_adhoc_cont_
manif_vrwe_eu_overv_cve_pract_2021_en.pdf; Daines et. al, “Spotlight: Violent right-wing extremism in focus,”
default/files/what-we-do/networks/radicalisation_awareness_network/docs/ran_brochure_violent_right_wing_
 extremism_in_focus_en.pdf
59 Ronen Hoffman, “Far Right Terrorism Similarities and Differences vs. Islamic Terrorism,” International Institute for
60 Peter Stone, “US far-right extremists making millions via social media and cryptocurrency,” The Guardian, 10
has spearheaded efforts to tackle online disinformation\textsuperscript{61} and promote media literacy,\textsuperscript{62} these should be fully incorporated into the counter-terrorism strategy rather than operating in parallel. However, the promotion of digital literacy skills should be thoroughly reflected upon, as this approach should also take into account the infrastructural design of social media platforms in order to be effective.\textsuperscript{63}

- We recommend that the EU’s Radicalisation Awareness Network (RAN) translates the most important research findings and best practices in the next counter-terrorism agenda, or ideally in the first EU far-right terrorism strategy. As part of this effort, we recommend that RAN create and maintain a central repository of far-right extremist mobilisation indicators to be used by all Member States in their domestic and transnational contexts, similar to the US Federal Government’s Mobilization Indicators booklet. Relatedly, we recommend that the EU counter-terrorism strategy draws upon findings conducted by RAN (for police, military, and prison staff) to implement a strategic review of individuals holding far-right extremist views in the military, as per European Commission recommendations for the Member States.

**In terms of the third pillar, enforcement:**

- Our primary recommendation for the US and EU strategies is to adopt legal and prosecutorial forces to the contemporary threat of far-right extremism, rather than solely relying upon pre-existing tools designed for countering Islamist terrorism. Relatedly, we recommend guidelines that protect personal privacy based on human rights and the rule of law. Protecting public safety should not come at the expense of guarding against potential abuse of overreach in prosecutorial and legislative reforms, despite different legal systems in the US and EU.

- Further, the EU can aim to foster stronger connections and cooperation between Member States through multi-agency responses in incorporating equal screening and vetting requirements of ties to far-right extremism in military personnel in order to protect national security.

**Finally, in the fourth pillar, building resilience:**

- We recommend that the EU should develop a long term response beyond risk management, and include more comprehensive social, cultural, and political aspects of resilience. Taking these crucial steps will help rebuild public trust and legitimacy towards national and EU governance, especially during the Covid-19 pandemic, which has been exploited by far-right extremists to recruit and radicalise supporters,\textsuperscript{64} noted also by the UN’s most recent review of the Global Counter-Terrorism Strategy.\textsuperscript{65} This is equally applicable to the US, as outlined in the Strategy. Part of these efforts will include the cultivation of media and digital literacy skills in the long-term, in order to build resilience against dis/misinformation, which contributes to social polarisation.


\textsuperscript{64}Ofra Klein, “How is the far-right capitalizing Covid-19?,” Centre for Analysis of the Radical Right Insight blog, 10 April, 2020, \url{https://www.radicalrightanalysis.com/2020/04/10/how-is-the-far-right-capitalizing-covid-19/}

Bibliography


Global Internet Forum to Counter Terrorism, “Governance,” https://gifct.org/governance/#government


Bibliography


About the Authors

Eviane Leidig

Dr. Eviane Leidig is a Research Fellow in the Current and Emerging Threats programme at ICCT. Her research focuses on far right extremism, gender, and online recruitment, radicalisation, and propaganda. Her regional expertise includes India, North America, and Europe. Eviane is also an affiliate at the Center for Research on Extremism (C-REX) at the University of Oslo; an Associate Fellow at the Global Network on Extremism & Technology (GNET) based at the International Centre for the Study of Radicalisation, King’s College London; and was a founding member of the Centre for Analysis of the Radical Right (CARR).

Charlie van Mieghem

Charlie van Mieghem is the Communications Officer at ICCT. Charlie has a Master’s degree in Crisis and Security Management (MSc) at Leiden University, The Hague and graduated cum laude. Her areas of expertise include the prevention of radicalisation and countering violent extremism, in particular far-right extremism.