Emerging Insights

Near-Sighted on Far-Right Financing
Why we Need a CTF Rethink

Stephen Reimer
ACKNOWLEDGEMENTS

An early draft of this paper was presented at the March 2022 Experts Symposium on Right-Wing Extremism, hosted by the Centre on Hate, Bias and Extremism at Ontario Tech University in Oshawa, Canada. The author would like to thank Henry McKeever, MA candidate in Conflict, Security and Development at the University of Exeter, for providing research support for this paper.

EXECUTIVE SUMMARY

Extremism and terrorism motivated by far-right ideologies has captured the attention of policymakers and much of the public as an urgent threat to peace, security and democracy across much of the Western world. This has not escaped the notice of practitioners of counterterrorism financing (CTF), many of whom see the far right as a natural extension of the global terrorist-financing threat. Although there is enthusiasm for immediately and directly applying CTF tools and responses to far-right fundraising and related financial activities, the ability of the CTF regime to suitably respond to this threat has been largely assumed. Through an analysis of the operational and organisational financing behaviours of the contemporary far right, this paper finds this financing threat to be largely incompatible with the CTF regime and identifies several shortcomings in the regime as it stands.

The vast majority of far-right violence emits meagre financial signals before an attack is carried out, which is incongruous with a CTF regime that depends on financial institutions to spot overt red flags in transaction data. Further, the CTF regime’s reliance on terrorism designations and resultant sanctions to financially isolate groups is at odds with the far right, whose organisational structures are unprecedentedly fluid and adaptable to such restrictive measures. In the absence of clearer direction from states, the private sector (especially operators of online platforms) has responded to pressure to independently ‘cut off’ perceived far-right ideologues and agents from accessing their services. Although laudable in their intention, such responses have precipitated several adverse consequences, including the spoiling of opportunities to collect financial intelligence on individuals and networks that could feed into more effective disruption efforts.

In recalibrating the CTF regime to make it more suitable for the far-right threat of today, this paper makes the following recommendations:

• To increase the likelihood of pre-attack financial signals being identified by financial institutions and used for preventative purposes, states should broaden public–private collaboration in the form of multi-agency ‘fusion cells’ involving social services, health, education, security intelligence services and financial institutions for real-time intelligence sharing on persons of interest.
• To maximise the near-term effectiveness of far-right terrorism designations for disrupting finance, states should provide their private sector (particularly financial institutions) with detailed lists (including names and identifying information) of real or legal persons linked to designated far-right groups to aid implementation.

• In recalibrating their national CTF regimes to meet the threat posed by the far right, states should reclaim authority and safeguard freedom of expression by denying private sector actors a free pass to make decisions, largely on the basis of reputation, about what constitutes violent extremism, as opposed to merely distasteful ideology.

• In building CTF regimes fit to combat far-right financing, states should include oversight mechanisms to forestall the abuse of anti-financial crime measures for authoritarian ends. Responding to far-right mobilisation using financial tools could also set dangerous precedents for authoritarian onlookers if not done transparently.

INTRODUCTION

The global counterterrorism financing (CTF) regime was devised in the immediate aftermath of 9/11 to respond to a particular problem: how to preclude transnational jihadist terrorism from using the global financial system to finance its operations. More than two decades later, the regime remains calibrated in this way, though the threat has changed substantially. Islamist extremism now contends with the far right for attention and CTF resources, illustrated by various countries’ recent decisions to include violent far-right groups on domestic lists of terrorist entities.¹ Terrorist designations of this sort indicate a growing, but possibly misguided, view among lawmakers in North America, Europe and the Oceania that the far-right threat can be confronted with the same CTF tools applied to the fight against jihadist terrorism.

Far-right violence is most likely to manifest in attacks by self-activating terrorists (SATs): individuals or small cells that are operationally autonomous in determining their targets and how attacks are prepared and financed. This is at odds with a CTF regime that relies on affiliation with designated groups and overt financial behaviours to identify and interdict terrorism financing (TF). A more thorough consideration of the extent to which the CTF regime is fit for purpose in light of the rising far-right terrorism threat is therefore needed.

A substantial body of research on the financing modalities of the contemporary far right already exists, which this paper does not endeavour to comprehensively summarise. Some of this work situates far-right financing within the context of preventing the financing of terrorism, but much of it is agnostic about this distinction. The aim of this paper is to scrutinise the CTF regime itself to see if it is a suitable mechanism for suppressing far-right financing. Being thus motivated by interrogating a potential response, the paper is unable to cover the totality of financial threats on display by the far right in all its forms.

Drawing on the behaviours and activities of North American, European and Oceanic far-right groups and agents up to the end of 2021, this paper highlights deficiencies of the global CTF regime that have been exposed through attempts at a direct application of existing countermeasures to the financing of far-right terrorism. Drawing on secondary sources, including policy reports, academic texts, news articles and think-tank research, it lays out an argument for why approaches to CTF interventions require a rethink if they are to adequately respond to terrorism premised on far-right ideologies. Recommendations for how this calibration should be carried out are also made.

TERRORISM, EXTREMISM AND THE FAR RIGHT

While the CTF regime provides states with clear obligations, it is silent on the matter of what constitutes terrorism itself. Aside from the universally applicable lists agreed to at the UN level, states are at liberty to maintain their own lists of terrorist entities and to judge by their own standards what may constitute terrorist activity requiring disruption. Central to making these determinations is striking the delicate definitional balance between terrorism and extremism: with extremism being the holding of a radical or fringe belief, and terrorism involving some use or threat of violence to achieve political change, often in alignment with extremist ideologies. This paper avoids the endless debate on the precise definitions of these related but importantly distinct terms, yet it must be pointed out that the CTF regime is itself agnostic as to the profile of the individuals or groups against which it is deployed. Therefore, the growing pace of far-right designations serves as an indicator of increased political concern over the threat of far-right ideologies. It should not be seen as a natural evolution of the CTF regime, but rather as a series of political choices made by sovereign states in response to what are, in their view, salient threats to security and society.

Far-right ideologies exceed mainstream conservatism and cover a broad spectrum of hateful views, typically characterised as a response to some sort of encroaching threat from, for example, non-white immigrants or migrants, as well as feminists and others perceived as seeking to upset traditional gender norms or family values. At their core is a rejection of multicultural, modern liberal democracy. Many far-right ideologies are known for taking anti-government, white supremacist, anti-Semitic, homophobic and neo-fascist positions, and typically condone and/or promote violence against ethnic minorities, law enforcement officers and politicians considered to oppose their views. Some of the most extreme far-right groups blame a perceived ‘societal degradation on factors such as widespread immigration and multiculturalism’, and see a solution in the form of triggering what they believe to be the inevitable breakdown of society through a global race war, a theory broadly known as ‘accelerationism’. Such ideologies have gained traction in numerous places, including Canada, the US, Australia, New Zealand and Europe to various extents, but notably in Western European countries such as Germany, the UK and Scandinavia. Given the demonstrable

3. Several UN Security Council committees responsible for overseeing asset freeze, travel ban and arms embargo measures imposed by the Council have been established concerning, inter alia, Islamic State, Al-Qa’ida and the Taliban.
capacities of far-right actors to undermine democratic and pluralistic values and to threaten and use violence to meet political ends, states in these regions have taken steps towards disrupting their financial networks using CTF tools.

A REGIME TO COUNTER THE FINANCING OF TERRORISM

The first doses of international attention applied to the issue of countering the financing of terrorism followed the Al-Qa’ida attacks on the US embassies in Tanzania and Kenya in August 1998.7 These events precipitated the conditions at the UN General Assembly that drove the adoption of the International Convention for the Suppression of the Financing of Terrorism in 1999, although the global CTF regime as it is known today did not emerge until the 9/11 attacks two years later.8 Member states of the Financial Action Task Force (FATF), the international standard-setter for anti-money-laundering (AML) measures, mandated that the body take on the fight against TF as well, issuing its nine Special Recommendations on CTF that member states would be measured against in the course of the established process of peer reviewing members’ compliance with the FATF standards.9

The FATF’s approach to CTF involved using AML obligations imposed on the private sector to also interdict flows destined for terrorist purposes. Reflecting how the 9/11 attacks were financed,10 this understanding of TF as a ‘corporate’ phenomenon assumed that terrorist groups raise funds through various sources – such as legitimate enterprise, criminality, state sponsorship and other donations – and then transfer those funds internationally through the formal financial system to fund attacks. To counter this, the CTF regime requires financial institutions to carry out compliance activities in two domains (summarised in Figure 1):

1. To **survey the financial behaviours of individuals** by using transaction monitoring tools to identify so-called ‘suspicious behaviours’ that may suggest TF activity, nearly always premised on a set of pre-established TF indicators or ‘red flags’, such as funds being transferred to an active conflict zone. Financial institutions are then

---

expected to file suspicious activity reports to a financial intelligence unit for further investigation.

2. To further the identification of terrorist groups and their members by carrying out customer due diligence checks on clients and ongoing screening of customer lists against relevant terrorism sanctions lists, such as the list produced by the 1267 Committee of the UN Security Council, which includes the names of Al-Qa’ida and Islamic State affiliates and financiers. Financial institutions are expected to freeze assets and report to government authorities should sanctions screenings yield a ‘hit’.

Figure 1: The CTF Regime


Note: BAFA = British Accounting and Finance Association, OFSI = Office of Financial Sanctions Implementation
The CTF regime – as it has been enshrined in the FATF standards, the 1999 Convention, and the resolutions and sanctions regimes of the UN Security Council – has been calibrated to the ‘corporate’, hierarchical understanding of TF for over 20 years, despite the TF landscape having shifted substantially almost immediately after the 9/11 attacks.\(^{11}\) According to Emilie Oftedal’s survey of jihadist plots carried out in Europe between 1994 and 2013, attacks reliant on international funding decreased sharply in the immediate aftermath of 9/11,\(^{12}\) likely in response to enhanced government surveillance and international cooperation succeeding in degrading the capabilities and command structures of organised groups.\(^{13}\) Groups instead began to prioritise stimulating autonomous operational activity, whereby plots would be mostly self-financed using banal, everyday sources of funds: a trend seen today among far-right attacks as much as those perpetrated by Islamist extremists.\(^{14}\) The question remains: can a CTF regime designed to identify and halt large international transfers be reformed to spot and interdict a very different set of financial behaviours?

**OPERATIONAL FINANCING AND THE SELF-ACTIVATING TERRORISM THREAT**

The EU’s policing agency Europol, in its 2020 European Union Terrorism Situation and Trend Report, stated that the most significant terrorist threat facing the continent ‘emanates from lone actors or small cells carrying out violence [of] their own accord without being directed by larger organisations’, regardless of ideological motivation.\(^{15}\) Similarly, the latest Public Report on the Terrorist Threat to Canada notes that individuals or groups inspired (and not directed) by violent ideologies and terrorist groups represent the principal terrorist threat to Canada,\(^{16}\) demonstrating the importance placed on SATs on both sides of the Atlantic.\(^{17}\)

---

17. A similar state of affairs is reflected in the 2022 US National Terrorist Financing Risk Assessment, and Australia’s Counter Terrorism Strategy 2022. See US
The author has chosen the term SAT to denote this common threat, given that other terms like ‘lone wolf’ or ‘lone actor’ are suboptimal and could be misleading, implying as they do that such actors operate in complete isolation. While this may be true in a few very rare cases – Anders Breivik, who was seemingly radicalised by his own ideology and self-financed his attack, may qualify as such18 – these actors are typically radicalised within an extremist milieu, feeding off propaganda disseminated by extremist groups and networks before exercising their operational autonomy and deciding to carry out an ideologically motivated attack of their own accord.19

This is clarified by the 2022 US National Terrorist Financing Risk Assessment in relation to the far right specifically, which emphasises that SATs ‘are more likely to carry out violent attacks in the United States than larger organizations’ that specialise in disseminating far-right extremist propaganda.20 The risk assessment goes on to state that SATs ‘often radicalize independently by consuming violent extremist material online and mobilize without direction from a violent extremist organization’.21 The same holds for European far-right SATs. For instance, before murdering his Chinese-born stepsister and attacking worshippers at an Islamic cultural centre, Philip Manshaus of Bærum, Norway, had been active on far-right message boards, posting before his attack ‘my time is up, I was chosen by Saint Tarrant after all’.22 He had also undergone a recruitment process to join the Nordic Resistance Movement, a transnational neo-Nazi movement with chapters across

---


21. Ibid.

Scandinavia, but his choice to attack before becoming a full member might suggest his impatience with the ‘mainstream’ far-right organisation.\textsuperscript{23}

Recent far-right SAT attacks across Europe demonstrate that attack planning expenses – such as reconnaissance and the procurement of weapons – or ‘operational terrorist financing’,\textsuperscript{24} are typically low, and therefore are financed by unextraordinary, seemingly legitimate means such as wage income, credit and loans, and personal donations.\textsuperscript{25} These methods do not leave notable financial footprints, nor do they draw the attention of financial institutions on the lookout for TF ‘red flags’.\textsuperscript{26} For example, when Stephan Balliet attacked a synagogue in the German city of Halle in 2019, he constructed his own weapons using everyday materials, including €50-worth of steel, a €20 telescope and 1,000 cartridge cases worth €25, all purchased in a hardware store and online.\textsuperscript{27} The transaction monitoring tools employed by most financial institutions would not identify such low-cost purchases of banal items as suspected TF. Other attacks may leave no financial trace whatsoever, such as that of Manshaus, who had pre-existing access to the firearms he used in his attacks, as did Tobias Rathjen, a registered marksman who legally owned the guns he used to attack two shisha bars in Hanau, Germany, in 2019.\textsuperscript{28}

The nature of far-right SAT attacks poses a challenge for the CTF regime in its current form, particularly as it pertains to countering operational TF. The ‘banal’ transactions that constitute far-right operational financing fail to raise suspicion within financial institutions, meaning there is no financial intelligence communicated to financial intelligence units and law enforcement agencies via suspicious transaction reporting. The purchase of everyday goods to construct, or be used as, a weapon, or rental of a vehicle that may be used in a ramming attack, will necessarily fly under the radar –


\textsuperscript{26} Ibid.

\textsuperscript{27} Spiegel Panorama, ‘Die wirre Welt des Attentäters’ ['The Confused World of the Assassin'], 14 October 2019; FATF, ‘Ethnically or Racially Motivated Terrorist Financing’, p. 28.

and rightly should, given that most vehicle rentals will be used for ordinary purposes. To raise the TF alarm for every such purchase would generate an inoperable rate of false positives, likely obfuscating true positives as a result. Reforms to the CTF regime will be needed to recalibrate tools for detecting suspicious financial behaviours to match the nature of far-right operational financing. SATs have been shown to leave some financial traces in their pre-attack activities, particularly for the most complex and ambitious plots, but these rarely present as ‘suspicious’ in the usual sense. Given this, new thinking on how financial intelligence is communicated from the private to the public sector will be necessary to spot operational financial indicators before an attack is committed.

ORGANISATIONAL FINANCING AND THE DESIGNATIONS DILEMMA

Compared with the limited scope of far-right operational financing, organisational financing is more wide ranging in its objectives, including the financing of maintenance costs, recruitment and training efforts, the living costs of operatives and producing and disseminating propaganda. To stem the flow of funds in support of terrorist organisations for such purposes, the CTF regime requires financial institutions to carry out customer due diligence checks to ensure that terrorism sanctions are enforced. However, the issue of terrorism designations presents a concerning dilemma for the efficacy of the regime to respond to the financing of far-right groups.

Under the current CTF regime, the toolbox of measures for responding to terrorism financing – such as asset freezes and travel bans – is only made available once a group has been designated as a terrorist organisation. That is to say, CTF measures cannot be applied against extremist organisations with unpalatable, yet not illegal, views and aims. The sanctions committees of the UN are the stewards of various sanctions lists with global applicability, including the 1267 Committee list of Al Qa’ida and Islamic State operatives and financiers. But there is no such consensus at the international level on far-right designations, so countries are left to consider this threat individually and sanction far-right groups in accordance with national procedures, which are disparate across North America, Europe and the Oceania. For example, the legislative arrangement in the US means that a far-right group in that country can only be designated a Specially Designated Global Terrorist under the provisions set out by Executive Order 13224, which require the group to be an agent of a foreign-based organisation, placing a major impediment

30. For analysis and recommendations on how potentially to reformulate established models of such information exchange, see ibid., pp. 33–35.
32. Because of the stipulation that a Specially Designated Global Terrorist must be based outside the country, the US has only designated one far-right group to date, the Russian Imperial Movement. See Nathan A Sales, ‘Designation of the
in the way of designating groups that are domiciled and operate solely in the US. Where countries are less encumbered, the decision whether or not to designate an extremist far-right group as a terrorist organisation typically hinges on their propensity for or incitement to violence, but these judgements are inherently subjective. For instance, the Nordic Resistance Movement was banned by the Supreme Court of Finland in 2020 yet the group’s chapter in Sweden remains a registered political party in that country.

In addition, a major challenge that arises from designating far-right groups as terrorist organisations is the ‘whack-a-mole’ problem, whereby a designated group may formally dissolve only to reform under a different name or alias. In numerous cases we see groups exhibiting remarkable adaptability, doing away with a listed name and brand while retaining the network of ideologically aligned individuals. This phenomenon can be seen most clearly in the UK, which has proscribed numerous far-right groups of the same origin:

- In December 2016 the UK listed National Action, a racist neo-Nazi group established in 2014 that glorified extreme violence for political and ideological ends.
- In September 2017, Scottish Dawn and NS131 were listed as aliases of National Action.
- In February 2020, System Resistance Network, the latest formulation of the network behind National Action, was added to the list.

The extremist network behind National Action and its various aliases has clearly been able to evade CTF countermeasures by dropping a group name upon its inclusion on a designations list. Shortly after National Action’s initial

---

33. Jason M Blazakis, ‘Can We Call the Proud Boys Terrorists?’, Slate, 4 February 2021.
34. To be clear, the Nordic Resistance Movement was not designated as a terrorist organisation in Finland. The Supreme Court ruled that the group be disbanded as it contravened Finnish association law by, among other things, being supportive of violent acts by its members and disseminating propaganda deemed hateful to ethnic minorities. Nonetheless, the point remains that there is no consensus between even closely aligned countries on what constitutes propensity to violent extremism in designation decisions. See Daniel Sallamaa and Tommi Kotonen, ‘The Case Against the Nordic Resistance Movement in Finland: An Overview and Some Explanations’, University of Oslo Center for Research on Extremism, 2 November 2020, <https://www.sv.uio.no/c-rex/english/news-and-events/right-now/2020/the-case-against-the-nordic-resistance-movement.html>, accessed 19 December 2022.
36. See Home Office, ‘Proscribed Terrorist Groups or Organisations’.

listing, one leader sent an email to members stating that ‘we are shedding one skin for another… these are exciting times’. This ‘whack-a-mole’ response to terrorism designations would appear to be in stark contrast to the effect of designations on other groups such as Al-Qa’ida and Islamic State, who retain their name and brand. This is not to say that proscribing far-right organisations is a useless practice. The Proud Boys indicated that they suffered financial difficulties after being designated a far-right terrorist organisation by Canada in 2021, claiming to ‘not [be] funded by the rich’. The group’s voluntary dissolution several months after the designation will likely have limited the threat posed by the group in the short term, as its members reconvene under some different organisational formulation. Further, designating far-right groups that have an international footprint can support targeted intelligence sharing between allies on common financing trends. In view of this, it would appear that terrorism designations are a necessary condition for opening the CTF toolbox, but are not in and of themselves a sufficient means of countering far-right organisational financing.

THE PRIVATE SECTOR STEPS UP/STEPS IN

Regardless of designation status, the private sector is increasingly being pressured to respond to the activities of far-right extremist organisations, pressures that are ceded to for reasons of mitigating reputational risk. However, these responses may generate their own negative unintended consequences. With a dearth of national far-right terrorism designations globally, some online platforms have opted to compile their own designations lists, such as Facebook’s ‘Dangerous Individuals and Organizations’, which features far-right student associations and music groups that have not been designated as terrorist organisations by any government. Facebook’s content moderators are required to flag and remove posts that ‘provid[e] direct (fundraising, donation-drive, etc.) or indirect (money laundering, accounting or banking services, etc.) financial support to an organization [on the list]’.

Deplatforming accounts altogether is an increasingly popular tactic adopted by the private sector to respond to the use of their services by the far right. Following the so-called ‘Unite the Right’ rally in Charlottesville, Virginia in

40. The Intercept, ‘Facebook Dangerous Individuals and Organizations List (Reproduced Snapshot)’, 12 October 2021.
2017, and the attack on the US Capitol on 6 January 2021, several far-right fundraising campaigns found themselves deplatformed from mainstream crowdfunding sites like GoFundMe and Kickstarter. Major payment services providers, including PayPal, Stripe, Apple Pay and Google Pay, refused to process payments made to alternative crowdfunding platforms such as Hatreon and MakerSupport, following initial waves of deplatforming. Removing selected content deemed to be at odds with a platform’s business philosophy is another tactic employed, often justified by a platform with reference to its community standards that prohibit content expressing hatred based on protected characteristics such as race or gender, or content encouraging violence. Amazon’s Community Guidelines are a typical example.

While typically well-meaning, these private sector interventions come with probable adverse consequences, chief among them being undesirable platform migration, whereby deplatformed individuals or organisations migrate towards less mature and less capable platforms to continue their fundraising or propaganda dissemination activities. This was seen during the ‘Freedom Convoy’ protests in Ottawa, Canada, in February 2022. Following the decision by GoFundMe to cease support for campaigns linked to the movement, supporters quickly pivoted to rival GiveSendGo to continue fundraising efforts. GiveSendGo is a much smaller firm than GoFundMe, with just 25 employees working remotely, and is infamous for facilitating campaigns for far-right causes and groups, including the Proud Boys.

Though difficult to prove, prominent voices, including blockchain analytics firm Elliptic and the FATF itself, judge that it is deplatforming from online crowdfunding and payment platforms that has driven the far right’s inclination to fundraise among supporters using cryptocurrencies. Whether or not this is the true motivation is debatable: many have speculated that the decentralised nature of virtual assets is ideologically attractive to far-right actors, who tend to be inherently suspicious of formal

---

Designating far-right groups that have an international footprint can support targeted intelligence sharing between allies

---

42. ABC News, “‘Unite the Right” Rally in Charlottesville Turns Violent”, 11 August 2017.
45. Amazon.co.uk, ‘Community Guidelines’.
financial institutions and organs of state. Nonetheless, this displacement of financial activity into more opaque territory is undesirable from a disruption point of view, because of the shortage of virtual asset expertise in national law enforcement agencies. Indeed, while transactions may be traceable, until staffing issues within the public sector are rectified, the blockchain can be expected to remain an under-surveyed domain for far-right financing.

Further, while the private sector will find it tempting to mitigate reputational risk and promote the public good by taking down extremist content and banning its proponents from their platforms (and will very likely face pressure to do so from fellow users), this risks cutting off intelligence-collection opportunities. Tracking donations made to crowdfunding platforms or posts made on social media sites can provide valuable financial and social media intelligence to law enforcement, which in turn could use that intelligence to map networks of associates or plan for more effective disruption of activities in future.

The current response to far-right organisational financing poses several challenges. Because of its adverse secondary effects, including platform migration and impacts on intelligence gathering, the current private sector response is not an adequate insurance policy against far-right extremism and terrorism. Nonetheless, the CTF regime itself will be similarly incapable without more designations of far-right groups, notwithstanding the shortcomings of this approach and the likelihood of groups evading sanctions by reforming under new aliases.

**CONCLUSION**

The global CTF regime and the FATF standards underpinning it were crafted to respond to a unique terrorist threat which only partially resembles the threat now posed by far-right extremism and terrorism. By analysing trends in far-right operational and organisational terrorism financing in North America, Europe and the Oceania, this paper identifies several deficiencies in the current response:

- Challenges in detecting financial behaviours indicative of attack planning.
- Inadequate means of transmitting financial intelligence from private to public sectors.
- Limited effectiveness of designating far-right terrorist groups.
- Adverse consequences of the private sector’s own responses.

---

48. See Jason Blazakis, ‘Far Right Online Financing and How to Counter it’, Global Center on Cooperative Security Policy Brief, August 2022, p. 3.
However, consider also whether the CTF regime itself is the ideal framework through which to design responses to the financing of terrorism and other security threats. Just as the far right has come to compete with jihadist terrorism and extremism for CTF attention and resources, in the near future, terrorism may come to play second fiddle to security threats posed by state adversaries and their proxies, a possibility that appears all the more likely following the full-scale Russian invasion of Ukraine in February 2022. In this context, there could be value in investing in threat finance capabilities that are oriented towards directly ensuring security, independent of the crime-prevention orientation of current AML/CTF controls and standards.\textsuperscript{51} Assessing the far right through a threat finance lens has the additional benefit of lessening dependence on a clear-cut definition of terrorism, which so often beleaguers responses to blatantly hateful and violent acts. If determined in a pre-defined, transparent and lawful manner, the financing of extremism, which falls short of terrorism but is still considered a threat to democracy or security, should be met with the same responses as proscribed terrorist groups. In many ways, the incongruence of the far right with the CTF regime may serve as a wake-up call to states for how to rethink their overall posture towards the financial dynamics of all threats to peace, security and democracy.

RECOMMENDATIONS

The CTF regime requires a rethink, and its measures must be recalibrated to meet the threat posed by far-right extremism and terrorism, in terms of both operational and organisational financing. Several recommendations stem from the main findings of this paper and should be taken on board at the national level in an effort to advance that recalibration and enhance the effectiveness of efforts to counter far-right financing in a human rights-compliant manner.

1. **Broaden public–private collaboration in the form of multiagency ‘fusion cells’ for real-time intelligence sharing on persons of interest.**\textsuperscript{52} Far-right SAT attack planning activities rarely present in financial transaction data alone, meaning that reliance on red flags and other indicators will either yield few results or, more likely, an inoperably high rate of false positives. Joining up intelligence streams across the public and private sectors – including from social services, health, education, security intelligence services, and financial institutions – will offer a better chance of identifying preparatory SAT attack activity.

2. **Provide the private sector (particularly financial institutions) with detailed guidance on how to effectively implement far-right terrorism designations.** Because of the ‘whack-a-mole’ problem,


\textsuperscript{52} This recommendation is relevant for the wider self-activating terrorism financing threat and stems from interviews conducted for the author’s prior research. See Reimer and Redhead, ‘A New Normal’, p. 35.
whereby designated groups dissolve and reform with a new public persona, designations are likely to be most effective in disrupting financial channels soon after they are announced. National authorities should provide the private sector with detailed lists (including names and identifying information) of individuals and corporate or charitable entities linked to designated far-right groups to aid in effective sanctions screening and subsequent asset freezing.

3. **Reclaim authority and safeguard freedom of expression.** Recalibration of the CTF regime to meet the threat posed by the far right should be conducted with restraint to safeguard civil liberties. Some private sector actions to counter far-right extremism and terrorism, such as Facebook’s Dangerous Individuals and Organizations policy, give a free pass to large social media companies and other platform operators to make decisions of their own accord about what constitutes violent extremism, as opposed to merely distasteful ideology. From a civil liberties perspective, it is concerning that such decisions may be made on the basis of a private company’s concerns about reputation and profitability, particularly if such quasi-designations systems offer no course for redress for those who believe they have been wrongly sanctioned. Unintended consequences of the present situation should be recognised when adapting the CTF regime in response to a threat whose harms to society are multifaceted and pernicious, particularly when compared with those of transnational jihadism.

4. **Forestall the abuse of anti-financial crime measures for authoritarian ends.** Responding to far-right mobilisation using financial tools may also set dangerous precedents for authoritarian onlookers if they are not transparent. For example, to disperse the Ottawa ‘Freedom Convoy’, the Canadian government resorted to co-opting the AML/CTF framework to freeze the assets of convoy supporters, an inappropriate use of asset-freezing powers to address not financial crime, but a public-order issue that had got out of hand. Such tactics have also been used by autocratic-leanings regimes to quell, for example, police brutality protests. A CTF regime fit to combat far-right financing should have oversight mechanisms to prevent such overreach and, by extension, the inadvertent legitimisation of authoritarian tactics to erode free expression.

53. In October 2020, the #EndSARS protest movement in Nigeria was severely disrupted after the country’s central bank ordered financial institutions to freeze the accounts of protest organisers without warning. See Stephen Reimer, ‘The Wrong Way to Truck Along’, *RUSI Commentary*, 22 February 2022.
ABOUT THE AUTHOR

Stephen Reimer is a Research Fellow in the Centre for Financial Crime and Security Studies at RUSI. He specialises in countering the financing of terrorism and threat finance generally. His recent work has focused on self-activating terrorism finance in Europe, the exploitation of new technologies for terrorism financing, assessing the risk of terrorism financing abuse in the not-for-profit sector, and the national security threats posed by illicit finance. He is also interested in corporate transparency and the unintended human rights impacts of the Financial Action Task Force standards.
About RUSI

The Royal United Services Institute (RUSI) is the world’s oldest and the UK’s leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today’s complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

The views expressed in this publication are those of the author(s), and do not necessarily reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.