Report on the emerging patterns of misuse of technology by terrorist actors

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Report on the emerging patterns of misuse of technology by terrorist actors

Council of Europe

French edition:

Rapport sur les modèles émergents de détournement des technologies par les acteurs terroristes

All other correspondence concerning this document should be addressed to the Directorate General Human Rights and Rule of Law, F-67075 Strasbourg Cedex, France
E-mail: dgi-cdct@coe.int

Cover design and layout: Publications and Visual Identity Division, Council of Europe

Photo: Shutterstock

Printed at the Council of Europe

Contents

Abbreviations

AI: artificial intelligence

AMF/CFT: anti-money laundering and countering financing of terrorism

CAD: computer-aided design

CBRN: chemical, biological, radiological or nuclear

CDCT: Council of Europe Committee on Counter-Terrorism

CFT: countering financing of terrorism

IEDs: improvised explosive devices

ISIL: Islamic State of Iraq and the Levant

ISKP: Islamic State Khorasan Province

ISWAP: Islamic State's West Africa Province

GCTF: Global Counterterrorism Forum

GIFCT: Global Internet Forum to Counter Terrorism

GNET: Global Network on Extremism and Technology

PKK: Kurdistan Workers' Party

Foreword

Terrorist and violent extremist groups and networks are increasingly using new technologies to advance their criminal activities by organising, financing, perpetrating and broadcasting attacks. These actions threaten our security and our democratic way of life. In a world where each technological advancement can be misused by terrorists and violent extremists, it is important to identify their usage patterns to help identify and implement effective countermeasures. This publication does just that by exploring why and how these groups and networks use technology, and the impact on the current terrorist landscape. It provides concrete recommendations for practitioners and policy makers.

This publication was developed as part of the Council of Europe Counter-Terrorism Strategy (2023-2027), with support from the German Federal Foreign Office. Under the auspices of the Council of Europe Committee on Counter-Terrorism (CDCT), Mr David Wells contributed to its development as an independent expert. Special thanks to practitioners from Council of Europe member states and representatives of the European Union Agency for Law Enforcement Cooperation (Europol), the Financial Action Task Force (FATF) and the Global Internet Forum to Counter Terrorism (GIFCT), whose insights helped shape the findings and conclusions.

Executive summary

Although the misuse of new technologies by terrorist actors has been a major concern for some time, the capabilities offered by (and the availability of) a range of new and emerging technologies – including gaming platforms, unmanned aerial systems (UAS), artificial intelligence (AI) and 3D-printed weapons – have heightened these fears even further.

An analysis of how and why terrorists adopt new technologies suggests that it remains highly context specific, with the extent and speed of innovation affected by internal factors (for example strategic, structural and individual factors) and external factors, particularly relationships, resources and the effects of counter-terrorism. In combination, these factors can encourage or inhibit the adoption of new technologies by terrorist actors, resulting in significant variations in the adoption and use of key technologies of concern.

Terrorist actors in or affecting Europe have adopted (or are beginning to adopt) many of these technologies. Social media platforms, small or micro platforms, terrorist-hosted websites and gaming or gaming-adjacent platforms are all playing critical roles in the radicalisation and recruitment process. Emerging technologies used in this process include the decentralised web, the dark web and, most recently, generative AI.

Although many terrorist attacks in Europe use a low-tech modus operandi, technology plays a key role in their preparation, planning and subsequent promotion. Propaganda and instructional material – typically stored and shared online – play a prominent role in shaping attack targets and methodology. For example, the emergence of 3D-printed weapon usage by terrorist actors in Europe has been fuelled by instructional materials developed by an active online subculture. Other far-right online subcultures have also encouraged the live-streaming of attacks and sharing of manifestos online.

Terrorist actors in Europe use a range of licit and illicit activities to fund their attacks and radicalisation and recruitment activities, some of which (but not all) require the use of new technologies. These include mobile payment systems, online exchanges and wallets, crowdfunding, peer-to-peer online funds transfers and the solicitation of donations on social media platforms. Simultaneously, terrorist actors outside Europe, notably ISIL (Islamic State of Iraq and the Levant)/Daesh, are increasingly encouraging donations via virtual assets, driving a rise in the presence of virtual assets in European terrorist financing arrests and prosecutions.

Interviews with national, regional and international experts identified lessons learned and good practices when responding to terrorist misuse of new technologies. These include reducing the lag between terrorist exploitation of new technologies and counter-terrorism responses to it (through horizon scanning exercises and greater information sharing), the criticality of multistakeholder approaches, the importance of identifying and managing human rights-related risks, and the benefits of greater strategic clarity, which can lead to a focus on desired outcomes, rather than the steps required to reach them.

Introduction

The Council of Europe Counter-Terrorism Strategy 2023-2027[1] identified the increased abuse of technology for terrorist purposes as one of its key areas of focus, citing the use of new technologies in terrorist recruitment, planning, financing and execution of attacks. Activity 1.4 of the strategy called for the production of an analytical report on emerging patterns of misuse of technology by terrorist actors, in order to support member states in identifying the main usage patterns, vulnerabilities and risks associated with these developments, and to implement the actions needed to monitor, disrupt and intercept terrorist activity. During its 12th plenary meeting on 14 May 2024, the Council of Europe Committee on Counter-Terrorism (CDCT) approved the initial outline of the report and tasked its independent consultant, David Wells, to produce a preliminary draft report for presentation at its 13th plenary meeting in November 2024.

The following report is primarily based on an extensive research phase, which included a review of a diverse range of academic literature and reports from a variety of national, regional and international institutions (including the Council of Europe) with a focus on terrorism and new technologies. This literature review was supplemented by interviews with key experts from six different national and international institutions, each of whom has been actively involved in countering terrorist use of technology in different capacities. These interviews were conducted remotely and on a non-attributable basis with a focus on developing a better understanding of the effectiveness of the different countermeasures used to address the misuse of different new technologies and identifying lessons learned and good practices to inform future responses.

The data collection and analysis have been synthesised into the following study, which is comprised of this introduction, a short section exploring the broader context relating to terrorism and new technology, and three substantive sections exploring the following points.

- Why terrorists adopt new technologies?
- How new technologies are influencing the current terrorist landscape in (and affecting) Europe?
- Counter-terrorism responses to new technologies: lessons learned and good practices.

An analysis of the information and insights gathered across the research and interview phases has informed the development of a limited set of recommendations for potential follow-up actions by the Council of Europe and its member states on how to strengthen counter-terrorism efforts and mitigate these risks.

1. Council of Europe Committee on Counter-Terrorism (CDCT), Council of Europe Counter-Terrorism Strategy (2023-2027), CM(2023)2, 8 February 2023.

Context

Technology has been misused by terrorists throughout history, acting as a force multiplier that has enabled them to project strength far beyond their actual size and instil fear at odds with the actual threat they pose. From the invention of dynamite in the 19th century[2] to tentative experimentation with generative AI in 2024,[3] terrorist misuse of technology (and how best to respond to it) has been perhaps the most consistent counter-terrorism challenge.

Over the past decade, the capabilities offered by, and availability of, a range of new technologies has increased at an even greater pace. Although many of these technologies have provided governments with significant benefits (or have the potential to), including in the field of counter-terrorism, their actual or potential misuse by terrorists and violent extremist actors – and the speed with which this occurs relative to the often slow integration of new technologies within policy and operational responses – has been a major concern for practitioners, policy makers and the broad array of entities involved in counter-terrorism today.

This was first recognised by the United Nations Security Council in its Resolution 2129, adopted in 2013, which noted the "nexus between terrorism and information and communication technologies, in particular the Internet" and their use to incite, recruit, fund or plan terrorist acts.[4] This framing, and in particular the specific focus on terrorist use of the internet, has driven a series of subsequent initiatives and activities, including multiple Security Council resolutions,[5] elements of the Council of Europe's Counter-Terrorism Strategy (2018-2022)[6] (including its subsequent "Report on emerging terrorist threats in Europe"[7]), public–private initiatives such as the Global Internet Forum to Counter Terrorism, activities by civil society organisations (such as the Christchurch Call) and the Global Counterterrorism Forum's (GCTF) Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online.[8]

More recently, there has been a broadening of this focus to include the challenges presented by the misuse of a range of new and emerging technologies.[9] In some cases, the exploitation of these technologies by terrorists and violent extremists has already taken place and is having operational effects (inside and outside Europe). These include the use of virtual assets and crowdfunding to raise and move funds, terrorist radicalisation and recruitment on gaming and gaming-adjacent platforms, the use of unmanned aerial systems to conduct reconnaissance, film propaganda and conduct attacks, and the use of 3D-printed weapons in several terrorist plots. In other examples, such as the misuse of generative AI and virtual or augmented realities for propaganda or operational purposes, or the potential risks posed by cyberterrorist activities, the focus has been primarily anticipatory, driven by concerns at the potential (or very early) consequences of their misuse.

Simultaneously, although terrorists and violent extremists are misusing new technologies, they are also exploiting a range of existing, well-established technologies to conduct their activities. Indeed, in some cases, they have actively pursued "low-tech" solutions to evade the attentions of authorities (for example through the use of knives or vehicles as weapons, or use of hawalas and money mules for financial transactions), with the former particularly prominent in the European context. In the regions or countries currently most affected by terrorism, notably in multiple regions of Africa, low-tech approaches are often the default, with recruitment and radicalisation activity often taking place offline, and ageing, conventional weaponry and improvised explosive devices (IEDs) the primary way in which attacks are conducted.

2. Hammes T. X., "Terror and technology: from dynamite to drones", *War on the Rocks*, 4 September 2020.
3. Wells D., "The next paradigm-shattering threat? Right-sizing the potential impacts of generative AI on terrorism", Middle East Institute, 18 March 2024.
4. Resolution 2129 (S/RES/2129) was adopted by the United Nations Security Council on 17 December 2013. The full text is available here.
5. These include resolutions with requirements relating to the collection of digital evidence (for example Resolution 2396 (2017)), countering terrorist narratives (Resolution 2354 (2017)) and countering the financing of terrorism (Resolution 2462 (2019)).
6. See, for example, Activity 1.2 "Preventing and countering terrorist public provocation, propaganda, radicalisation, recruitment and training on the internet", Council of Europe Counter-Terrorism Strategy (2018-2022), CM(2018)86, CDCT, 4 July 2018.
7. The report is available here.
8. The recommendations are available on the GCTF website, with the subsequently developed toolkit (to operationalise the recommendations).
9. See, for example, the Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes, United Nations Security Council Counter-Terrorism Committee, 29 October 2022.

One potential explanation for this apparent discrepancy between the nuanced, context-specific role played by new technologies in terrorist activities and the major focus on new and emerging technologies by national, regional and international authorities, both in terms of their assessment of terrorist risk and how new technologies are integrated within their response, is what terrorism scholar Bruce Hoffman has referred to as the "technological treadmill".[10] The simultaneous risk and reward posed by new technologies has led to both terrorists and counter-terrorism feeling under pressure to continually innovate and adopt new technologies, or risk being overtaken technologically by their adversary.

This pressure can be hypothetical but it can also be informed by past experiences, which in the context of counter-terrorists and new technologies are not necessarily positive. For example, many of the operational and policy frameworks that counter-terrorism actors operate under, particularly in the European context, were developed in response to the rapid rise of the so-called Islamic State in Iraq and the Levant (ISIL/Daesh) and the exodus of foreign terrorist fighters (FTFs) to conflict zones in the Middle East from 2012 onwards. Terrorist misuse of the internet was often central to this mobilisation, with ISIL/Daesh using a range of mainstream internet platforms and applications to radicalise and recruit thousands of individuals[11] and dominate the global media and policy agenda.

It seems likely that the extent to which authorities were taken by surprise by ISIL/Daesh's initial mastery of cyberspace – and, most importantly, how long it took to develop a holistic response to counter it – has left counter-terrorism professionals understandably reluctant to underestimate the risks posed by terrorist misuse of other new technologies. This type of mindset (which also applies in a range of other policy contexts) was well summarised in July 2024 by a Microsoft executive as: "The greatest risk is not that the world will do too much to solve these problems. It's that the world will do too little. And it's not that governments will move too fast. It's that they will be too slow."[12]

The rise of ISIL/Daesh also rapidly increased the number of countries and regions affected by terrorism, creating a truly global organisation with an external operations capacity and the possibility of new potential synergies between a diverse group of FTFs[13] in conflict zones. Simultaneously, the growing far-right terrorist threat has exhibited increasingly transnational tendencies, such as the exchange of tactics and techniques. This has made it more difficult for policy makers and practitioners to assume (or hope) that particular trends, challenges or methodologies would be confined to particular national or regional contexts.

As a result, the emergence of new technologies with potential terrorist use cases or the experimentation with new technologies by terrorist actors in one national or regional context has frequently resulted in authorities in different national, regional and international contexts committing significant resources in an effort to understand how feasible or replicable these terrorist use cases are and identify potential responses.

10. Hoffman B. (2006), *Inside terrorism*, Columbia University Press, New York, pp. 252-253.
11. Barrett R. et al., "Foreign fighters in Syria", The Soufan Center, New York, June 2014.
12. Smith B., "Protecting the public from abusive AI-generated content", Microsoft, 30 July 2024.
13. Some estimates suggest that FTFs from more than 110 countries travelled to join ISIL/Daesh. See, for example, Barrett R., "Beyond the caliphate: foreign fighters and the threat of returnees", The Soufan Center, New York, October 2017.

Why terrorists adopt new technology

Despite these understandable fears, the adoption of new technologies by terrorist actors has continued to be context specific, with clear differences in the rate of adoption and the types of technology misused by terrorists in different national and regional contexts. To assist Council of Europe member states in taking a more context-specific and nuanced approach to assessing the risks posed by new and emerging technologies, this section will seek to analyse how and why terrorists innovate (including through the use of new technologies) and identify the factors that determine whether specific technologies receive limited, piecemeal or widespread adoption. It will conclude with two case studies that demonstrate how this analytical framework can be applied in practice.

Terrorist innovation: overview

Over the past two decades, researchers have examined how best to conceive of and categorise terrorist innovation. One of these scholars, Adam Dolnik, focused on how to define innovation, which he characterised as the "introduction of a new method or technology or the improvement of an already existing capability". This can encompass both radical innovation (the use of brand-new tactics or technology) or incremental innovation (an improvement or modification of a tactic).[14] Others, notably Gill et al.,[15] also emphasised the distinction between creativity – identifying solutions to problems – and innovation, which is the effective implementation of such strategies. This is a critical distinction, because although creativity is a difficult process to encourage and foster in and of itself (in any organisation or movement), implementing the solutions identified during this process can often be even more complicated. It is also the part of the process which counter-terrorism interventions can most easily disrupt.

Other scholars have explored the different types of innovation in the terrorist context, which Martha Crenshaw defined as tactical (adopting new technologies for the same objectives), strategic (identifying new objectives) and organisational (organisational structure or recruiting processes).[16] Crenshaw also argued that the ultimate purpose of terrorist innovation is to maintain the element of surprise, in light of adaptation by state actors to the actions of terrorist groups. This is particularly salient given that some scholars have estimated that 90% of terrorist organisations die out or disappear within their first year of existence;[17] one reason for the survival of the remaining 10% is their ability to adapt, innovate and be creative against the more substantial state powers against which they fight.[18]

14. Dolnik A. (2009), *Understanding terrorist innovation: technology, tactics and global trends*, Routledge Contemporary Terrorism Series, London and New York.
15. Gill P. et al., "Malevolent creativity in terrorist organizations", *The Journal of Creative Behaviour*, 4 June 2013.
16. Crenshaw M., "Theories of terrorism: instrumental and organizational approaches", *Journal of Strategic Studies*, 24 January 2008.
17. Since David Rapoport's widely cited claim in 1992, more recent studies have examined this data point and concluded that the actual figure is likely to be around 50%. See, for example, Philips B. J., "Do 90 percent of terrorist groups last less than a year? Updating the conventional wisdom", *Terrorism and Political Violence*, 6 September 2017.
18. Gill P. et al., "Malevolent creativity in terrorist organisations", *Journal of Creative Behaviour*, 2013.

The adoption of new technology is just one element of this approach to innovation, with new technologies contributing towards both radical and incremental innovation at the tactical level and leading to both strategic and organisational innovation. Although there has been a significant amount of research on the issue of terrorist creativity and innovation (including the role of technology), the primary focus has been on the tactical level, with a particular focus on attack methodologies. More recently, there has been a growing awareness of the importance of other tactical innovations,[19] especially the response of terrorist actors to government and private sector countermeasures on larger social media platforms, which has typically led to innovation with different smaller online platforms.[20]

Given the demonstrable role that technology has also had in enabling new organisational objectives for terrorists (for example how ISIL/Daesh used social media and encrypted applications to recruit on a truly global scale) and to a lesser extent, strategic ones, it is vitally important to explore the factors that encourage or inhibit this innovation. This paper will therefore build on these models to create a framework that helps develop a shared understanding of why terrorists have or have not adopted various new technologies.

It is first useful to consider the different functions required for terrorists and terrorist groups to operate successfully. These can be broadly distilled down to the following three functions.

- Resources: this can cover each aspect of the financial cycle, encompassing the raising, moving, storing and spending of funds, including the acquisition of the equipment/material required for the second and third functions.
- Communication: this covers both internal communication (for co-ordination and instruction) and external communication (for recruitment, polarisation and publicity).
- Attacks: this ranges from devising a plan and conducting reconnaissance to conducting the attacks themselves, and the future use of attack activity for publicity or propaganda purposes.

These three functions are of course interlinked. To use a technological example, drones have been used by terrorist groups for reconnaissance and to conduct attacks, but also to create propaganda which has, in turn, helped to raise funds.[21] Post-attack external communication (for example media coverage of the attack and/or related propaganda) may also drive fundraising or recruitment (both positively and negatively) and the carrying out of inspired attacks by sympathisers or supporters. These overlaps and connections demonstrate both the need to address terrorist use of technology holistically – rather than with a focus on the use of a specific technology within one function – and the potential complexity of understanding how and why a particular technology is adopted by terrorists.

Terrorist innovation: internal factors

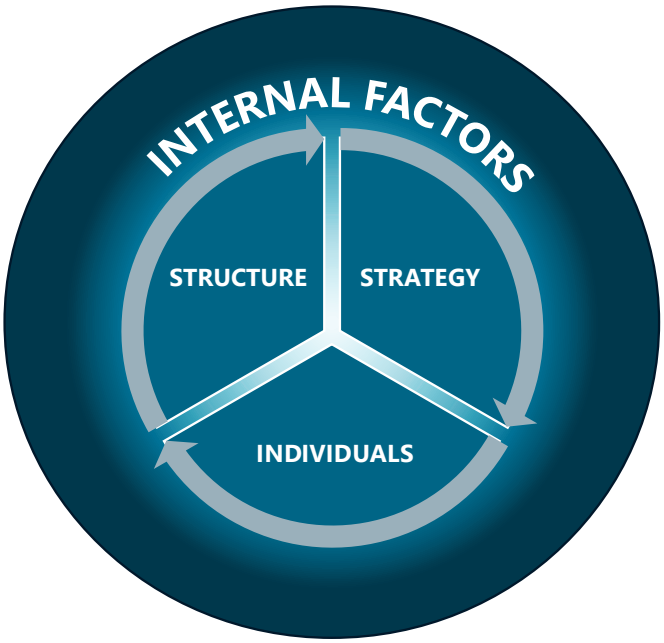
Turning then to the factors affecting innovation by terrorists, these can be both internal and external, with a significant amount of interplay between the two. There are multiple interconnected, internal factors, which have been grouped together for brevity, including the following.

- **Strategic factors**: these include the broad compatibility between organisational or movement-wide strategic goals or ideologies and the adoption of a particular innovation (including the use of technology). A key aspect of this compatibility is the balance between, or hierarchy of, different priorities, including speed, effectiveness, cost and likelihood of detection. Terrorist actors in particular have to balance secrecy (to avoid intervention/prevention) with relevance and impact (which requires a sacrifice of secrecy).[22] For example, al-Qaeda's approach to potential new recruits after the 11 September 2001 attacks (post-9/11) typically prioritised secrecy and avoiding state intervention through a comprehensive vetting system[23] at the expense of the potential impact offered by a greater number of recruits. In contrast, from 2013 onwards, ISIL/Daesh chose a much greater degree of openness to new recruits (in-person and online), potentially compromising its secrecy and making it more vulnerable to penetration by intelligence agencies but maximising its potential reach.

19. Kfir I., "Terrorist innovation and online propaganda in the post-caliphate period", Social Science Research Network, 4 November 2019.
20. Amarasingam A., Maher S. and Winter C., "How Telegram disruption impacts jihadist platform migration", Centre for Research and Evidence on Security Threats, 8 January 2021.
21. United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), "Greater efforts needed to address the potential risks posed by terrorist use of unmanned aerial systems", May 2019.
22. Kfir I., op. cit.
23. Joscelyn T., "Spying on al Qaeda", *Long War Journal*, 10 May 2012.

- **Structural factors**: these strategic choices often affect the type of structure used by a terrorist group or movement, which in turn, also affects the extent to which, and how, it will innovate. Research has shown that hierarchical, structured groups are not intuitively creative, with Salafi-jihadist groups often conservative in nature,[24] but that simultaneously, they have consistently prioritised (and indeed, been leaders in) tactical innovation in relation to attack methodology. In contrast, innovation in loosely structured or unstructured terrorist movements, particularly those based around online rather than physical communities (including the far-right, leaderless resistance model), can be driven from the bottom-up, which can make them more responsive to opportunity-driven change.
- **Individual factors**: regardless of structure, there are of course a wide range of individual factors affecting innovation. Traditionally, academics and government agencies have placed a significant emphasis on the role of leaders within terrorist organisations,[25] including in relation to their attitudes towards change and innovation and their ability to learn from the past experiences of themselves and others. However, these factors also apply to lone actor terrorists and those connected to more loosely defined movements. Other characteristics particularly relevant to innovation in the technology context include creativity, levels of expertise, the level of attachment to or trust in a particular technology and age.

Figure 1 – Internal factors affecting terrorist innovation



24. Winter C., Maher S. and al-Tamimi A. J., "Understanding salafi-jihadist attitudes towards innovation", International Centre for the Study of Radicalisation, 19 January 2021.
25. Long A., "Assessing the success of leadership targeting", *CTC Sentinel*, November 2010.

Terrorist innovation: external factors

These factors are of course interlinked and intersect with a range of external factors, which include the following.

- **Relationships**: relationships between different terrorist actors have historically helped drive terrorist innovation by enabling the sharing of technology, techniques and knowledge of countermeasures. One example of this type of direct relationship was the travel of three alleged members of the Irish Republican Army (IRA) to Colombia in 2001, who were subsequently convicted of providing explosives training to the Revolutionary Armed Forces of Colombia (FARC).[26] More recently, the internet has made this sort of information increasingly accessible without requiring (or risking) a direct relationship between different terrorist actors. This has included access to instructional material[27] on both the surface and dark web (particularly in relation to IED construction), but also broader lessons learned relating to the successes and failures of others, including why and how planned attacks were identified and prevented. This is particularly pertinent in the context of lone actor attacks, which are often defined by the absence of direct, personal and operational relationships between the attacker and others. Finally, relationships between terrorist groups and governments can also be a key driver of innovation, as they enable the sharing of technology, knowledge and other resources. Research into the use of UAS by non-state armed groups has particularly highlighted this element, with the majority of successful attacks using UAS involving groups who have relationships with state actors.[28]
- **Resources**: there are a broad range of resources that affect terrorist innovation with new technologies. Money is the most critical, given that it enables the acquisition of other components critical to terrorist innovation including equipment, recruitment and paying the salaries of terrorist group members. However, access to funds is not in and of itself a guarantee of access to the resources required for successful innovation with new technology, particularly given the level and types of expertise that might be required. One example of this is al-Qaeda's long-running but ultimately unsuccessful attempt to conduct chemical, biological, radiological or nuclear (CBRN) terrorist attacks, which included the recruitment of scientists, construction of laboratories and aborted attempts to produce or acquire CBRN materials in several different countries.[29] This broader question of the accessibility of both a particular technology and the associated expertise required to adopt it has been highlighted by researchers as a key factor in how terrorists approach innovation with new technology, particularly in relation to its relative complexity and cost.[30]
- **Counter-terrorism**: finally, and perhaps most importantly, all terrorist innovation occurs within the context of national, regional or international counter-terrorism and preventing or countering violent extremism (P/CVE) efforts, all of which vary in terms of the approaches taken and their effectiveness. Terrorists within permissive operating environments have more freedom to innovate than those in contexts with effective counter-terrorism actors. Simultaneously, they often also have less need to innovate, due to having ready access to weaponry and explosives, and the ability to raise, store and move funds unhindered. The counter-terrorism environment can also affect the targets of terrorist attacks, with target hardening efforts potentially displacing terrorist activity to softer targets that only require "low-tech" methodologies. For example, although stringent security measures have been slowly expanded throughout airports globally in response to terrorist attacks and plots, airports have remained a recurring target of terrorist attacks, with the focus for attacks shifting outside the securitised zones.[31]

Successful counter-terrorism disruptions and prosecutions can also raise awareness among terrorist actors of investigative techniques used by authorities to detect and disrupt terrorist plots, driving further innovation to evade these efforts. This can relate to both vulnerabilities with existing technologies used by terrorist actors (for example certain communications platforms or devices being accessible to intelligence and law-enforcement agencies) or broader vulnerabilities within their existing modus operandi that can be addressed by the use of new technology (for example the use of encryption[32] or offline mapping applications to avoid being tracked

26. Taylor L., "Colombia revokes amnesty it granted to alleged IRA bomb-making trio", *The Guardian*, 16 December 2022.
27. Europol, "Crackdown on material designed to 'educate' future terrorists", 21 December 2023.
28. See, for example, Rassler D., "Going the distance: the emergence of long-range stand-off terrorism", *CTC Sentinel*, February 2024.
29. Mowatt-Larssen R., "Al Qaeda's pursuit of weapons of mass destruction", *Foreign Policy*, 25 January 2010.
30. Veilleux-Lepage Y., Daymon C. and Archambault E., "Learning from foes: how racially and ethnically motivated violent extremists embrace and mimic Islamic State's use of emerging technologies", Global Network on Extremism and Technology (GNET), 7 June 2022.
31. See, for example, the 2016 attacks at Brussels and Istanbul airports, which targeted passengers located before security and outside the terminal buildings.
32. Mascellino A., "End-to-end encryption sparks concerns among EU law enforcement", *Infosecurity Magazine*, 23 April 2024.

by law enforcement). It is of course very difficult to prove that a particular policy or counter-terrorism response is the direct cause of a specific terrorist innovation (or, indeed, that a counter-terrorism response prevented a course of action). However, it is clear that counter-terrorism actions do lead to terrorist reactions – both positive and negative – particularly with regard to innovation and new technologies.

Figure 2 – Internal and external factors affecting terrorist innovation

Terrorist adoption of new technology: case studies

To give a sense of how these different factors affect terrorist adoption of new technology, the paper will explore two case studies in which new technologies with apparent benefits for terrorist actors have been adopted to a greater or lesser extent, and at different speeds.

Case study 1: the misuse of unmanned aerial systems (drones)

Concerns regarding the potential misuse of UAS by terrorist actors in Europe have been raised since ISIL/Daesh successfully weaponised UAS in Iraq and Syria in 2016 and 2017, merging commercial off-the-shelf technology with low-tech components and other technological add-ons.[33] At its height, the ISIL/Daesh UAS programme was reportedly responsible for more than one hundred attacks in Iraq in one month,[34] resulting in European Union officials repeatedly warning about the risks of drones being used to attack European cities.[35] Despite UAS technology becoming increasingly accessible and affordable, and frequent references in terrorist propaganda to the use of UAS to target Europe (including during the 2024 Olympics in Paris),[36] UAS have yet to be adopted by terrorist actors in or targeting Europe. There are a range of internal and external factors that help explain why this has been the case (to date). It is worth noting that Türkiye has also witnessed the use of paragliders/paramotors by terrorist actors in the attack against the Tece police house in the Mezitli district of the Mersin province in the autumn of 2024. Although differing in many respects from UAS, they represent another aerial attack vector that terrorist actors might seek to exploit in the future considering that they are relatively inexpensive and easy to obtain and assemble.

Internal factors

From a strategic risk perspective, UAS still score relatively poorly in comparison to other attack methods, particularly in relation to cost and effectiveness (given the sizeable challenges relating to reliably weaponising drones), and uncertainty over whether the purchase of drones or UAS-related components or conducting practice flights might raise red flags with authorities. From a structural perspective, hierarchical groups are more likely to drive long-term innovation in attack methodologies, whereas the present threat environment in Europe is dominated by lone actors and small cells that typically lack this formal structure. Indeed, a counter-terrorism analyst from a European member state recently shared that their greatest concern related to terrorist groups with UAS programmes, as they allow for dedicated resources, expertise and funding and benefit from facilitation networks that enable access to components or commercial drones.[37] However, individual factors point towards the potential adoption of UAS in the future, with the European terrorist landscape typically dominated by younger individuals who are likely to be tech-savvy and potentially have pre-existing familiarity with UAS technology.

33. Rassler D., "The Islamic State and drones: supply, scale and future threats", Combating Terrorism Center at West Point, July 2018.
34. Sullivan B., "The Islamic State conducted hundreds of drone strikes in less than a month", *Vice*, 21 February 2017.
35. Martin N., "EU: terrorists could use drones for attacks", Deutsche Welle, 8 March 2019.
36. Courtney-Guy S., "ISIS warns of Eiffel Tower drone attack in chilling Paris Olympics threat", *Metro*, 10 June 2024.
37. Quoted in United Nations Office of Counter-Terrorism (UNOCT), "Global report on the acquisition, weaponization and deployment of unmanned aircraft systems by non-state armed groups for terrorism-related purposes", UNOCT Autonomous and Remotely Operated Systems Programme and Conflict Armament Research, March 2024.

External factors

Turning then to external factors, there are a multitude of opportunities for terrorist actors in (or targeting) Europe to learn indirectly from the experiences of other non-state actors who have successfully weaponised UAS. At this stage, there appears to be very limited evidence of direct relationships between Europe-based terrorist actors and groups or individuals with this type of expertise, which would be critical in fast-tracking the weaponisation of UAS in Europe. However, understandable concerns have been raised about the spillover of methodologies and technology from current conflict zones.[38] Although access to expertise and know-how relating to the use of UAS and any countermeasures to prevent their misuse is already likely to be available, resources are likely to be a factor in the failure to adopt UAS, given the relative cost of UAS technology in comparison to the methodologies that are currently prevalent in self-funded attacks.

Finally, the prevalence of largely effective and comprehensive counter-terrorism approaches in Europe has created a difficult operating environment for groups or individuals seeking to innovate with weaponised UAS. For example, there are already restrictions in place regarding the use of drones around critical infrastructure and in particular urban environments, alongside EU-wide information-sharing initiatives and the ongoing testing of different counter unmanned aerial systems (C-UAS) technologies.[39] While there are concerns about the operational effectiveness of some of these measures – and about programmatic and policy-related activities that seek to address these challenges[40] – they may have influenced how terrorist actors perceive the likelihood of early detection and disruption of their UAS-related activities.

Clearly, these internal and external factors, and the broader strategic calculus of terrorist actors in Europe will not remain static. Potential drivers of change include further reductions in the cost of drones, the wider availability of instructional material regarding their reliable weaponisation, further terrorist propaganda encouraging their use in the European environment or high-profile UAS attacks in other contexts. However, the above framework does provide a useful way to assess the likelihood of the adoption of UAS (or other technologies) by terrorist actors, as well as identify barriers to their adoption that can be monitored to assess future risks and challenges.

Case study 2: virtual assets

Since Bitcoin was created in 2009, cryptocurrencies and other virtual assets have been widely used by a range of criminal actors, due to their perceived anonymity and the initial absence of the anti-money laundering and countering financing of terrorism (AML/CFT) requirements that are designed to flag suspicious transactions to government authorities. Given these apparent operational benefits – and the transnational nature of many terrorist movements which necessitates the movement of funds internationally – there have been long-standing concerns among the counter-terrorism community that virtual assets would be rapidly adopted by terrorists, with Canada taking measures as early 2014[41] to address the AML/CFT risks associated with virtual currencies.

Over the past 10 years, there has been a gradual uptick in the prevalence of virtual assets within counter-terrorism investigations, particularly over the past three to four years, but they are yet to have the type of effect envisaged by the US Navy in 2014 for example, which warned that "the introduction of virtual currency will likely shape threat finance by increasing the opaqueness, transactional velocity, and overall efficiencies of terrorist attacks".[42]

Internal factors

Although virtual assets appear broadly compatible with the strategic goals and ideologies of most terrorist actors in the European context, there remain issues regarding their effectiveness. This is due to their volatility – how quickly and regularly they fluctuate in value (particularly for coins that prioritise anonymity through a private ledger)[43] – the difficulties of converting virtual assets into cash in certain jurisdictions and the proven

38. Bell S., "West must adapt as drones become weapon of choice for military 'underdogs' and terror groups", *Sky News*, 3 February 2024.
39. European Commission, "Communication from the Commission to the Council and European Parliament on countering potential threats posed by drones", 18 October 2023.
40. Unmanned Airspace, "European Commission announces funding for the EUR 71 million E-CUAS programme", 17 May 2024.
41. Canadian Broadcasting Company, "Budget 2014: Bitcoin, charities face scrutiny to prevent money laundering", *Yahoo News*, 12 February 2014.
42. Cohen B., "U.S. Navy preparing Bitcoin battalion", *Bitcoin Magazine*, 24 April 2014.
43. Alexander A. and MacDonald T., "Examining digital currency usage by terrorists in Syria", *CTC Sentinel*, March 2022.

ability of public and private actors to trace transactions back to individual users. From a structural perspective, the terrorist landscape in Europe also appears well suited to the adoption of virtual assets, with the lack of well-defined, hierarchical groups encouraging a bottom-up approach, driven by individuals. However, a significant percentage of terrorist attacks in Europe are self-initiated and therefore self-funded,[44] using long-standing methods including legal business structures, the collection of donations, membership fees and criminal activities.[45] In contrast, most of the virtual asset activity identified to date – and indeed, most of the individuals arrested in 2022 for terrorist financing activity – has been external in nature, with funds sent to terrorist organisations based outside the EU, not used for Europe-focused activities or attacks.[46]

As such, the gradual shift towards virtual assets has been primarily driven by external factors, namely innovation by external terrorist actors, with the growth occurring once terrorist groups like ISIL/Daesh and its affiliates signalled their interest in, and ability to, receive funds via virtual assets. Finally, the young, tech-savvy nature of many terrorist actors, and the increasing mainstreaming of a range of virtual assets, makes it likely that terrorist actors will have been exposed to the use (and pros/cons) of virtual assets in everyday life. This can make it difficult to determine whether virtual assets are present in counter-terrorism investigations because they are being used for terrorist purposes, or merely because terrorist actors are using virtual assets for non-terrorism related activities.

External factors

Given how mainstream virtual assets are and their continued use by a range of criminal actors, a wide range of direct or indirect sources and relationships can drive innovation by terrorist actors. Due to the relatively limited adoption by terrorist actors, and the widely diverging standards and approaches across different virtual assets and exchanges, there is perhaps a less clear "best practice" for terrorist actors to follow, and this is likely to result in divergent approaches to virtual assets. Resources appear to be a less critical factor for Europe-based terrorist actors, with the barrier for entry to virtual assets much lower than in the past (in terms of technical know-how). However, this is a greater issue for terrorist actors who might be recipients of virtual assets from Europe-based individuals, due to challenges relating to the presence of exchanges, currency fluctuation (both virtual and "physical") and challenges around converting virtual assets into cash,[47] with the related global infrastructure still relatively inconsistent.

Finally, counter-terrorism actions remain a significant inhibitor on the use of virtual assets, with successful counter-terrorism prosecutions (and other criminal prosecutions) in multiple jurisdictions demonstrating that many virtual assets are traceable, with nefarious transactions successfully tracked back to an individual user. Indeed, a June 2023 report by the Egmont Group of Financial Intelligence Units stated that one terrorist group had stopped using virtual assets for fundraising purposes due to "successful government efforts to identify and prosecute donors".[48]

In addition to these specific internal and external factors, the overarching context in which terrorist actors in Europe have been operating for the past five to six years helps further explain their relatively limited adoption of virtual assets. Lone actor or small cell terrorism that has been primarily internal in nature has predominated, due to both the territorial defeat of ISIL/Daesh (the previously dominant external terrorist organisation recruiting and mobilising European terrorist actors) and the growth of a far-right terrorist threat that prioritises a "leaderless resistance" model. Recent trends that point towards the increasing salience of external groups or conflicts on the terrorism threat level – in particular several attack plots in Europe linked to the Islamic State Khorasan Province (ISKP)[49] – suggest that this landscape could shift, with the potential for funds to be directed both into and out of Europe, using conventional or virtual methods, including to support more targeted attacks.

44. Reimer S. and Redhead M., "A new normal: countering the financing of self-activating terrorism in Europe", RUSI Europe, May 2021.
45. Europol (2023), *European Union terrorism situation and trend report 2023*, Publications Office of the European Union, Luxembourg.
46. Ibid.
47. Alexander A. and MacDonald T., "Examining digital currency usage by terrorists in Syria", *CTC Sentinel*, March 2022.
48. Egmont Group of Financial Intelligence Units, "Report on abuse of virtual assets for terrorist financing purposes", Information Exchange Working Group, June 2023.
49. Clarke C. P. and Webber L., "ISKP goes global: the world is not ready to confront a new international terror threat", *Foreign Affairs*, 1 August 2024.

How new technologies are affecting the current terrorist landscape in (and affecting) Europe

Following this exploration of how terrorists innovate using technology at a macro level – and two case studies examining how this works in practice – it is important to analyse how these different factors, and the interplay between them, have affected the current terrorist landscape in (and affecting) Europe. Given the dangers of generalising across different countries who are experiencing different threat types and are seeking to respond to them with variable resources and approaches, this section will try to be specific where possible, including by providing examples or case studies based on different national contexts. It will, however, draw together some broader, regional trends to allow for a clearer understanding of the current threat picture.

Terrorist communication and radicalisation

Sharing terrorist content

Although the drivers of radicalisation to terrorism remain complex – and affect individuals in both their online and offline lives – the European Union Agency for Law Enforcement Cooperation (Europol) has noted that "the use of technology and the internet (including social media platforms, instant messaging applications, online forums and video gaming platforms) continues to play a crucial role in the radicalisation and recruitment process of individuals and in spreading propaganda material".[50]

In the European context, although the specifics of where and how terrorist propaganda is stored and shared will vary depending on the ideology of the group or movement behind it, there remain key commonalities in terms of the types of new technologies exploited and the methodologies used to do so. These include relatively well-established technologies and methodologies. In particular, terrorists and violent extremists continue to seek to exploit major social media platforms, given that they offer them the widest possible audience for their propaganda and the greatest potential for their activity to go "viral".

However, the collaborative efforts of governments, civil society and the platforms themselves have ensured that it is now more difficult for terrorists to flourish on these larger platforms. For example, the EU's Terrorist Content Online Regulation requires hosting providers to remove terrorist content within one hour of being notified by a competent authority,[51] with sanctions for non-compliance potentially extending to a penalty of 4% of a platform's turnover. This is supported by Europol's EU Internet Referral Unit, which conducts quarterly Referral Action Days to identify terrorist content online and then refer the associated URLs to online service providers for removal.[52]

In parallel, many platforms are proactively identifying and removing content that is in breach of their own terms of service, including terrorist content. Thirty-two technology companies are now members of the Global Internet Forum to Counter Terrorism,[53] through which they have access to (and contribute to) a hash-sharing database. This contains the unique "digital fingerprint" of each piece of terrorist content that has been identified by GIFCT and its members, allowing members to either remove or prevent the content from being uploaded onto their platform. As a result of this database – and a variety of other machine-learning techniques used by different platforms[54] – it has become difficult for known terrorist content to be posted on most of the larger platforms. For example, of the millions of items of terrorist content removed by Facebook, approximately 98% is detected proactively by the platform.[55]

50. Europol (2023), *European Union terrorism situation and trend report 2023*, Publications Office of the European Union, Luxembourg.
51. See Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online for more information.
52. See, for example, Europol, "Crackdown on material designed to 'educate' future terrorists", 21 December 2023.
53. For a full list of members, see the GIFCT website.
54. Macdonald S., Mattheis A. and Wells D., "Using artificial intelligence and machine learning to identify terrorist content online", Tech Against Terrorism Europe, 17 January 2024.
55. Ibid.

These external factors (that is, counter-terrorism efforts) have undoubtedly significantly influenced the extent to which terrorist actors have been required to innovate with new technologies for their radicalisation and recruitment activities. As a result, they are now using an increasingly diverse range of platforms and applications to create, store and share terrorist content, with Tech against Terrorism identifying terrorist content on 187 different online platforms between November 2020 and January 2023, with 78 of these being small or micro platforms.[56]

Smaller platforms typically have more limited resources to moderate content of all kinds (and in some instances, are opposed to the concept of content moderation) and are also less likely to have established working relationships with law-enforcement agencies. This can again be due to resourcing issues, the novelty or limited nature of terrorist activity on the platform, the jurisdiction in which the platform is hosted and run, or the ideological persuasion of its owners. As a result, terrorist actors have been able to retain their online presence, albeit with a more limited audience.

Although these smaller platforms pose significant challenges, particularly in relation to file sharing and storage of content, there remains a persistent ecosystem of larger online apps and platforms that have been misused by terrorist actors for some time, but whose content moderation efforts and relationship with law-enforcement officials have been insufficient to deter terrorist misuse. Most prominent among these is Telegram, which has been widely used by terrorist actors of many ideological persuasions for much of the past decade,[57] and has over 900 million monthly users, making it one of the top ten most popular social networks globally.[58] More recently, X (formerly known as Twitter) has scaled back its content moderation efforts, allowing previously outlawed types of content on the platform (and, in some cases, promoting them) and welcoming back far-right accounts previously removed from Twitter for incitement.[59] As a result, X has once again become a home for terrorist and violent extremist users from across the ideological spectrum.

In addition to using platforms or apps hosted by other companies, some terrorists have also developed their own websites to host terrorist material, with Tech against Terrorism identifying nearly 300 terrorist or violent extremist-operated websites over a two-year period. This approach offers a stable and accessible space to host propaganda materials, recruit new members and raise funds,[60] with the websites also used to host instructional material that would be in breach of the terms of service of almost all online platforms.

The threat posed by terrorist-operated websites was targeted by Europol in June 2024, with a joint investigation culminating in the seizure of four servers in Romania, Ukraine and Iceland, and the referral of 13 websites to their service providers for removal.[61] National law-enforcement agencies have also targeted the individuals acting as administrators for the websites, with a British man responsible for running two far-right websites (but not creating the content they hosted) sentenced to seven years in prison in early August 2024 on four counts of disseminating a terrorist publication.[62]

Gaming and gaming-adjacent platforms

Another online ecosystem of increasing concern in the context of recruitment and radicalisation are gaming and gaming-adjacent platforms. This apparent shift towards different online spaces appears to have been driven by internal factors – particularly the non-hierarchical nature of the terrorist ecosystem in Europe and its relative youth – and the counter-terrorism pressures referenced above. The influence of indirect relationships driving terrorist learning is another external factor, in particular the high-profile live-streaming of the Christchurch and Buffalo terrorist attacks, which mimicked the visual style of first person shooter video games.[63]

There are a variety of ways in which terrorism can intersect or interact with the gaming ecosystem.[64] This encompasses mainstream games, which typically have an online component that enables peer-to-peer or group communication, and online gaming communities or channels in which gamers can live-stream their

56. Tech against Terrorism, "Patterns of online terrorist exploitation: TCAP insights", April 2023.
57. Tan R., "Terrorists love for Telegram, explained", *Vox*, 30 June 2017.
58. Dean B., "How many people use Telegram?", *Backlinko*, 17 July 2024.
59. Ingram D., "Verified pro-Nazi X accounts flourish under Elon Musk", *NBC News*, 16 April 2024.
60. Tech against Terrorism, "Terrorist operated websites: explainer", 7 August 2024.
61. Europol, "Europol-coordinated operation tackles the threat of terrorist-operated websites", 14 June 2024.
62. The UK Crown Prosecution Service, "Far-right extremist jailed for running racist websites used by international terrorists", 2 August 2024.
63. Schlegel L. and Amarasingam A., "Examining the intersection between gaming and violent extremism", United Nations Office of Counter-Terrorism, 6 October 2022.
64. For an overview of some of these concerns, and emerging responses to them, see "Conference summary: the abuse of livestreaming, gaming and virtual reality services and platforms by terrorist actors", Council of Europe Committee on Counter-Terrorism, November 2023.

activities and engage with followers and a broader community (including Steam, Twitch, DLive and Discord). Although these latter applications were originally developed for gaming purposes, they have evolved to more closely resemble the functionality of traditional social media or e-commerce platforms,[65] but without necessarily having the same content moderation capacities or relationships with law-enforcement officials.

Concerns about these potential vulnerabilities have been reinforced by the repeated use of gaming imagery or terminology in terrorist propaganda[66] (notably by ISIL/Daesh) – suggesting that terrorist groups or movements are aware of the affinity between their potential audience and the gaming world – and the gamification of terrorist activities themselves, particularly within the far-right community.[67] Violent extremists have also created video games of their own or customised levels for existing games, including by offering gamers the chance to recreate past terrorist attacks.[68]

In 2021, Europol noted the extent to which far-right propaganda was prevalent on gaming platforms, forums and channels as a "growing trend",[69] and this risk has been frequently echoed by other law-enforcement agencies (both inside and outside Europe),[70] particularly in the context of children being exposed to terrorist content. Despite this combination of potential vulnerabilities, demonstrable interest among terrorist actors in the gaming ecosystem, and widespread acknowledgement of the prevalence of hateful and violent attitudes and behaviour on gaming platforms,[71] there have been relatively limited concrete, operational examples of the use of gaming or gaming-adjacent platforms to conduct radicalisation and recruitment. However, with continued evidence of the targeting of children by terrorist groups of different ideologies across Europe, and the ongoing popularity of gaming and gaming-adjacent platforms among this demographic, this remains an issue of significant concern.

Emerging technologies

In addition to these relatively incremental innovations in how to use technology to recruit and radicalise, terrorists and violent extremists have also begun to experiment with newer technologies. These have included the use of the decentralised web (DWeb)[72] and the dark web to share and store propaganda.

Terrorists have also begun to use generative AI to create propaganda materials,[73] which offers them the ability to rapidly create terrorist content in a range of formats, styles and languages, potentially allowing them to more effectively target different demographics and segments of populations. There are also concerns that generative AI chatbots could be used to "outsource" the radicalisation process,[74] with the chatbot programmed to reinforce terrorist ideologies and promote disinformation, and able to do so in multiple languages, 24 hours per day. This risk is not entirely hypothetical, with a chatbot playing a role in encouraging a mentally unstable individual to conduct an attack against the UK monarch in December 2021 (although the chatbot had not been programmed for this purpose).[75]

To what extent terrorists utilise generative AI – and other emerging technologies such as the Metaverse – to radicalise and recruit will again be influenced by the internal and external factors outlined earlier in the report and, of course, the speed with which the technology continues to develop (and how that affects its accessibility and effectiveness). Countering any misuse may also require a shift away from a primary focus on the platforms where terrorists are sharing and disseminating propaganda and content, to also focus on how and where the content is being created. More broadly, given the centrality of technology to terrorist radicalisation and recruitment, member states should anticipate further innovations in which technologies are used, and how they are used.

65. Lakhani S., "Video gaming and (violent) extremism: an exploration of the current landscape, trends and threats", EU Radicalisation Awareness Network (RAN), 1 October 2021.
66. Dass R. A. S. and Singh J., "How IS exploits gamification of violence in bid to appeal to youths online during the pandemic", *M today*, 9 June 2021.
67. For more, see Lakhani S., White J. and Wallner C., "The gamification of (violent) extremism: an exploration of emerging trends, future threat scenarios and potential P/CVE solutions", EU Radicalisation Awareness Network, 7 September 2022.
68. Tech against Terrorism, "State of play: trends in terrorist and violent extremist use of the internet 2022", 19 January 2023.
69. Europol (2021), *European Union terrorism situation and trend report 2021*, Publications Office of the European Union, Luxembourg.
70. See, for example, *The Guardian*, "Online gaming platforms such as Roblox used as 'Trojan horse' for extremist recruitment of children, AFP warns", 3 December 2023.
71. Schlegel L. and Amarasingam A., "Examining the intersection between gaming and violent extremism", United Nations Office of Counter-Terrorism, 6 October 2022.
72. Bodo L. and Trauthig I. K.,"Emergent technologies and extremists: the DWeb as a new internet reality", GNET, 1 August 2022.
73. Borgonovo F., Bolpagni A. and Lucini S. R., "AI-powered jihadist news broadcasts: a new trend in pro-IS propaganda?", GNET, 9 May 2024.
74. Jowitt T., "Terrorism Tsar warns of AI chatbot radicalisation risk", Silicon, 5 January 2024.
75. Vaughan H., "AI chat bot 'encouraged' Windsor Castle intruder in 'Star Wars-inspired plot to kill Queen'", *Sky News*, 5 July 2023.

Terrorist attacks

Current modus operandi and instructional material

Technology has traditionally played a critical role in enabling terrorists to plan, conduct and publicise their attacks. For much of the decade following the 9/11 terrorist attacks, the predominant terrorist threat remained relatively complex attacks, often featuring improvised explosive devices and firearms, while the targets included transportation or public spaces with the hope of achieving a mass casualty event.

In contrast, the current terrorist threat in Europe is perhaps best characterised as predominantly low tech, with the past three Europol terrorism situation and trend reports (TESAT) emphasising the prevalence of rudimentary attack methods, including stabbing using bladed weapons, vehicle ramming and arson,[76] alongside fewer attacks or plots featuring IEDs and firearms.

A range of internal and external factors have combined to shift this threat environment over the past decade. These included changes in strategy by al-Qaeda – notably through its call for "Open Source Jihad", promoting local, self-initiated attacks through its *Inspire* magazine[77] – and subsequently ISIL/Daesh, when it asked its supporters to conduct attacks at home, rather than travel to Iraq and Syria. Both of these strategic shifts were driven largely by counter-terrorism efforts, which made it more difficult for both groups to plan and execute terrorist attacks outside their sphere of influence, including in Europe, and recognition that more sophisticated and complex terrorist plots were being detected and disrupted by authorities. Finally, far-right terrorist actors were also able to learn from these trends and have, to some extent, shifted their attack methodologies accordingly.

Although many current attacks and attack plots are low tech in their proposed modus operandi, that does not mean that they are necessarily low tech in their planning or in how propaganda is spread following a successful attack. In-group communications to plan attacks and conduct other activities are now typically encrypted, posing significant challenges for government authorities seeking to intercept and understand.

In the context of lone actor attackers, the ideological and operational inspiration is typically provided via propaganda and instructional material sourced online. However, recently, there has been growing evidence of a return to the type of directed plots that were prevalent during ISIL/Daesh's peak in 2015 and 2016, but this time connected to the ISKP. Authorities have prevented ISKP-linked attacks in Austria, France, Germany, Spain and Türkiye, leading to an assessment that the ISKP represents the greatest external threat to Europe. Some European member states have even drawn parallels to the ISIL/Daesh-driven terrorist threat landscape of 2015 to 2017.[78]

The recency of many of these plots (most of which have taken place in 2024) makes it difficult to determine to what extent they were directed or inspired by the ISKP, which technology (if any) was used for communication between the ISKP and the attackers in Europe, and what role technology was likely to play in the planned attacks. However, given the past success of the "virtual plotter" methodology[79] and the relative safe haven enjoyed by the ISKP (which can be a key driver of terrorist innovation), it is possible that, in the future, ISKP-linked attacks or plots may utilise a more sophisticated modus operandi, including in relation to attack technology.

Another critical way in which technology is contributing towards the current threat landscape is the prevalence of instructional materials online. This "how to" material can cover a wide range of activities, including constructing homemade weaponry, bomb-making, the targeting of critical infrastructure or how to avoid detection when planning a terrorist attack.[80]

The threat posed by this type of material is significant and long established, dating back to early bomb-making manuals, the *Anarchist cookbook* and the *Turner diaries*.[81] More recently, al-Qaeda in the Arabian Peninsula launched its *Inspire* magazine in January 2010, containing a wealth of instructional material. This included its infamous "Make a bomb in the kitchen of your mom" article which was subsequently followed to build bombs used in the terrorist attack on the Boston Marathon in 2013.[82] *Inspire* magazine's strategic ethos – which was

76. Europol (2021), *European Union terrorism situation and trend report 2021*, Publications Office of the European Union, Luxembourg.
77. Black I., "Inspire magazine: the self-help manual for al-Qaida terrorists", *The Guardian*, 24 May 2013.
78. United Nations Security Council, Thirty-fourth report of the Analytical Support and Sanctions Team pursuant to resolutions 1526 (2004) and 2253 (2015), 22 July 2024.
79. Gartenstein-Ross D., Clarke C. P. and Shear M., "Terrorists and technological innovation", Lawfare, 2 February 2020.
80. Europol, "Terrorist 'how to' guides – focus of latest Europol Referral Action Day", 3 July 2020.
81. Reed A. and Ingram H. J., "Explaining the role of instructional material in AQAP's *Inspire* and ISIS' *Rumiyah*", Europol, 26 May 2017.
82. Esposito R., "Exclusive: government doc shows how closely Boston Marathon bombers followed al Qaeda plans", *NBC News*, 26 April 2013.

described by researchers as "lowering the barriers of entry to terrorism, with the aim of fostering a do-it-yourself ethos resulting in terrorist behaviors"[83] – has subsequently been embraced by ISIL/Daesh and a range of other terrorist groups or movements, including across the far-right.

These instructional materials are stored and shared across a range of different platforms, including the dark web and on Telegram, notably within the Terrorgram Collective, a neo-fascist Telegram network that was recently proscribed as a terrorist organisation by the UK.[84]

3D-printed weapons

A particular area of concern are instructional materials relating to the production of 3D-printed weapons. In the decade since Defense Distributed released the digital files for the world's first almost entirely 3D-printed firearm, there have been rapid improvements in the design, reliability and effectiveness of 3D-printed weapons,[85] fuelled by extensive innovation and experimentation from an online network of both malicious actors and gun hobbyists.[86]

Unsurprisingly, these developments have also attracted the interest of terrorist actors, including those in Europe, where counter-terrorism and broader law-enforcement efforts have generally made it difficult for malicious actors to reliably source firearms. This has been one factor in the prevalence of IEDs and more recently bladed weapons or vehicle ramming attacks in terrorist attacks in Europe.[87]

Simultaneously, a range of other internal and external factors have encouraged this interest, particularly among the far-right. These include the prevalence of young individuals who spend a long time online in a largely unstructured movement, and the opportunities to learn from direct and indirect relationships within these online communities, including the example set by the Halle attacker in 2019, whose arsenal included 3D-printed components.

These factors, alongside decreases in the cost of 3D printers, have resulted in a significant increase in the terrorist threat posed by 3D-printed weapons, particularly in the five years since the Halle attack, with arrests or seizures made across Europe, including in Germany, Iceland, the Netherlands, Spain, Sweden, the UK and Finland.[88] In the latter example, when police arrested a four-man far-right cell who had planned racially motivated attacks targeting critical infrastructure, they recovered semi-automatic weapons and other weapon components produced using a 3D printer. Their subsequent conviction for a range of terrorist and firearms offences marked the first terrorism conviction in Finland connected to the far-right.[89]

The weapons seized by Finnish police included four FGC-9s, a semi-automatic hybrid pistol that is assessed to be one of the easiest semi-automatic homemade firearms to construct, can be produced for approximately US$500 and requires no controlled firearm parts, thereby circumventing European gun regulations.[90] Indeed, a recent report by the EU-funded Project INSIGHT concluded that "3D-printed firearms pose the greatest potential challenge to national and international small arms controls".[91]

Simultaneously, the manuals, computer-aided design (CAD) files and instructions for design and manufacture of weapons like the FGC-9 are readily available on online platforms.[92] This makes the risks posed by 3D-printed weapons both a technological problem in and of itself, and deeply connected to the availability of instructional material on the surface web across a range of online services (highlighting the need for effective content moderation) and on the dark web.

83. Lemieux A. F. et al., "*Inspire* magazine: a critical analysis of its significance and potential impact through the lens of the information, motivation, and behavioral skills model", *Terrorism and Political Violence*, 14 January 2014.
84. Farrell-Molloy J., "The proscription of Terrorgram as a terrorist organisation in the UK: insights from the Independent Reviewer of Terrorist Legislation", Vox-Pol, 26 June 2024.
85. Veilleux-Lepage Y., "Printing terror: an empirical overview of the use of 3D-printed firearms by right-wing extremists", *CTC Sentinel*, Combating Terrorism Center at West Point, June 2024.
86. GIFCT Red Team Working Group, "Risks and challenges in online communities for 3D-printed firearms among extremists and terrorists", 20 September 2023.
87. See, for example, Pauwels A., "Prevention of gun-, knife-, bomb- and arson-based killings by single terrorists", in Schmid A. P. (ed.) (2021), *Handbook of terrorism prevention and preparedness*, International Centre for Counter-Terrorism, ICCT Press Publication.
88. Vallance C., "3D printed guns: warnings over growing threat of 3D firearms", *BBC News*, 9 November 2022.
89. *The Guardian*, "Finnish neo-Nazis used 3D printer to make guns in preparation for 'race war'", 31 October 2023.
90. Dass R., "3D-printed weapons and the far-right: the Finnish accelerationist cell", GNET, 6 October 2023.
91. Schroeder M. et al., "Privately made firearms in the European Union", Project INSIGHT, Small Arms Survey, December 2023.
92. Dass R., op. cit., GNET, 6 October 2023.

Concerningly, there are potential connections between the risks posed by 3D printing and another technology-driven terrorist threat, drones (UAS), with a British student convicted of preparing acts of terrorism in September 2023 following the seizure of a drone and a 3D printer capable of producing parts for it. The suspect, who was subsequently sentenced to life imprisonment, had planned to weaponise the drone with chemical weapons.[93] As covered in case study 1, although the adoption of UAS in the European context has been relatively limited to date, they remain an attack vector of significant concern for counter-terrorism authorities.

Publicity

Finally, technology has become progressively more important to the ability of terrorists to publicise their attacks, including as they are occurring. Again, there are a range of internal factors responsible for this shift. From a strategic perspective, the ability for ISIL/Daesh to quickly claim responsibility either directly – or through videos or statements produced and sometimes released by the attacker(s) in the European context – allowed them to reinforce their claim to be "remaining and expanding". Organisationally, the far-right's "leaderless resistance" also encouraged bottom-up innovation, including in relation to the content associated with an attack (which has included live-streamed attacks and, frequently, manifestos) and how and where it was shared.

From an external perspective, the latter activity by the far-right often overtly displayed the extent to which terrorist actors can learn from and inspire each other, including by referencing previous attacks and attackers, emulating imagery and employing similar methods. The popularity of the live-streaming of terrorist attacks is also a reflection of the resources available to lone actor attackers in the European context, both in terms of the very accessible technology needed for live-streaming, but also their familiarity with live-streaming (and its associated benefits) from non-terrorist contexts, due to their age and time spent online. Finally, counter-terrorism efforts online that have limited terrorist access to the larger social media platforms have forced terrorist actors to look for more innovative ways to achieve virality, maximising the impact of their attack.

Terrorist financing

Current trends

The financing of terrorist activities in (and from) Europe has also been subject to some of the same internal and external factors (particularly pressures from AML/CFT measures) and the broader shifts to the terrorist threat landscape. Terrorist financing has also become increasingly dependent on a range of different technologies.

Post-9/11, the threat model that most concerned law-enforcement authorities was the top-down flow of funds from al-Qaeda leadership to operational cells across the world, following the pattern established by the 9/11 attacks themselves. However, subsequent research suggested that due at least in part to counter-terrorism pressures, the attacks marked the zenith of such a model. Instead, al-Qaeda shifted away from directed attacks funded and planned by terrorist actors located outside Europe, towards propaganda activities that could stimulate self-activated attacks, which were typically self-funded.[94]

Subsequent data from a range of research studies and national or regional government reports have provided valuable insights into sources of funding for these types of attacks and plots. These include legitimate income, credit or loans, state benefits, personal donations, the sale of personal effects and the use of the proceeds from illicit activities; while there has been some evidence of the use of virtual assets to purchase items as part of the attack preparation cycle, they do not appear to have been used as a source of funding[95] (for more, see case study 2). Although the above picture appears to point towards a relatively low-tech CFT threat landscape, most of these sources of funds – and how they are then used to purchase weapons, other components or conduct reconnaissance activities – still typically intersect with the mainstream financial system and require (to some extent) the use of technology to access, share and spend the funds.

Of course, the terrorist financing picture in Europe extends beyond the conducting of terrorist attacks, with funds required to support a wide range of terrorist activities (particularly radicalisation and recruitment). Sources of these funds similarly include legal business structures, the collection of donations – notably those collected at in-person events – or membership fees, and criminal activities. The sale of merchandise, videos, publications

93. Page T., "Mohamed Al Bared: student jailed for life for building IS drone", *BBC News*, 22 December 2023.
94. Reimer R. and Redhead M., "A new normal: countering the financing of self-activating terrorism in Europe", RUSI Europe, May 2021.
95. Ibid.

and tickets for events (for example concerts), including on e-commerce platforms, are other ways used by terrorist actors to raise funds,[96] and this is particularly prominent among far-right groups and movements.

However, the primary focus of CFT activities in Europe, at least with regards to arrests and convictions, has been on the flow of funds from Europe to terrorist groups located elsewhere, notably Syria. For example, in 2020, Austria, Germany, Ireland, the Netherlands, Spain, Sweden, Switzerland and the UK all arrested, charged or convicted individuals for terrorist financing offences related to the transfer of funds outside Europe, to groups including ISIL/Daesh, and the Kurdistan Workers' Party (PKK).[97] In 2022, EU member states reported 14 arrests for terrorist financing offences, all of which related to terrorism inspired by ISIL/Daesh or al-Qaeda, with the majority accused of raising funds for terrorist organisations located outside the EU.[98]

This focus on funds leaving Europe for terrorist groups is due to a range of factors, including shifts in attack and organisational strategy by both al-Qaeda and ISIL/Daesh, the continuing resonance of ISIL/Daesh activities in Syria for terrorist actors in Europe – particularly in relation to ISIL/Daesh-associated women and children who remain in detention, many of whom are European or have close ties to Europe – and the continued impact of counter-terrorism and CFT measures on the ability of terrorist groups to move funds into Europe.[99]

Although this has a less direct, short-term impact on the European threat landscape, the presence of well-resourced terrorist groups operating from relative safe havens with direct ties to Europe remains a significant concern. In parallel, although the threat posed by far-right terrorism has increased significantly over the past five years, its leaderless resistance model has made it more difficult for member states to proscribe, designate or ban far-right terrorist groups, which is often a key pre-cursor to meaningful CFT action at the national level.

Virtual assets and emerging methodologies

As a result, innovation with new technologies with regard to terrorist financing has been primarily driven by the actions of these external terrorist actors, as opposed to those conducting fundraising activities and/or sending funds overseas from Europe. In the case of ISIL/Daesh and the use or receipt of virtual assets, despite increases in their ability to, and interest in, receiving virtual assets from 2020 onwards, there remain significant regional variations across its provinces and subgroups.

Although ISIL/Daesh Central primarily relies on cash couriers and the hawala network, other ISIL/Daesh provinces have taken a more diversified approach, with both the ISKP and the East and South Africa network notable for their growing (but still relatively limited) use of cryptocurrencies. In contrast, there is little evidence of the Islamic State's West Africa Province (ISWAP) or ISIL/Daesh groups operating in Mozambique and the Democratic Republic of the Congo using cryptocurrencies.[100] This variation is itself a reflection of a range of internal and external factors, with researchers pointing towards the importance of local conditions, including the presence of a developed cryptocurrency sector in the destination country, and a compelling reason to avoid conventional financial systems.[101]

There is some evidence that individuals in Europe are seeking to send funds to ISIL/Daesh using virtual assets. In February 2024, the Spanish authorities arrested a man who was alleged to have sent nearly €200 000 to ISIL/Daesh in cryptocurrency,[102] while in June 2024, the German authorities arrested an individual in part due to his transfer of nearly US$1 700 in cryptocurrency to an address linked to the ISKP.[103]

From a European perspective, this variation among terrorist groups (or subgroups) in their ability to receive and use virtual assets will affect the extent to which European terrorist actors will be able to send funds to terrorist groups overseas using this method. There are a range of reasons why an individual or group might be more inclined to send funds to the ISWAP ahead of the ISKP for example (including national or ethnic background, familial or friendship connections, or the impact/profile of their terrorist operations). It is possible that the readiness of one ISIL/Daesh "province" to receive funds using a particular technology (such as cryptocurrency), or their broader technological compatibility with potential terrorist funders in Europe, might also sway decision making in the future.

96. Europol (2023), *European Union terrorism situation and trend report 2023*, Publications Office of the European Union, Luxembourg.
97. Europol (2021), *European Union terrorism situation and trend report 2021*, Publications Office of the European Union, Luxembourg.
98. Europol (2023), op. cit.
99. One jurisdiction reported that terrorist groups have also sought to exploit natural disasters (such as earthquakes) to raise funds under the guise of "disaster relief".
100. Davis J., "The financial future of the Islamic State", CTC Sentinel, July/August issue 2024.
101. Ibid.
102. TRM, "Jordanian national arrested in Spain for Sending 200,000 Euros in cryptocurrencies to the Islamic State", 1 February 2024.
103. TRM, "German authorities arrest man suspected of sending cryptocurrency to ISKP", TRM, 13 June 2024.

There are a range of other new or emerging technologies used to transfer funds to regional or international terrorist groups, including mobile payment systems, online exchanges and wallets, crowdfunding, peer-to-peer online funds transfers and the solicitation of donations on social media platforms, including through the use of the "super-chat" functionality.[104] Again, although traditional methods to move funds (including cash, money transfer systems and hawala) remain predominant, each of these newer technologies has the potential to pose challenges to current CFT approaches, particularly as they can be used to diversify risk and/or in combination with each other.

104. "CTED's tech sessions: highlights on 'threats and opportunities related to new payment technologies and fundraising methods'", United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), 29 October 2022.

Counter-terrorism responses to misuse of new technologies

Lessons learned

To build on the understanding of how terrorists innovate with new technology, and how this is currently affecting the terrorist landscape in Europe, interviews were conducted with a range of national, regional and international experts. Each has significant, contemporary experience with combating terrorist use of new technologies in different contexts. During the interview process, they identified both good practices and lessons learned that might be more broadly applicable to countering new technologies in a counter-terrorism context in the future.

- **Slow responses**: multiple interviewees contrasted the speed with which terrorist actors were able to experiment with and adopt many new technologies, and how long it often took national, regional and international organisations to identify the potential risks this posed, before even considering how best to respond to them. While there was a recognition that the nature of terrorist actors meant that they were typically more flexible and agile than state ones, stakeholders felt that the gap between the two responses was too large.
- **Information-sharing challenges**: the transnational nature of the terrorist threat – often driven by technology – made it impossible for national services to manage the terrorist threat on their own, particularly given the (often significant) differences in the technical capabilities and resources at their disposal. However, interviewees identified recurring structural and organisational barriers to the effective and timely sharing of information between (and sometimes within) countries.
- **Information-access challenges**: terrorist use of technologies often exacerbated this challenge by requiring states to navigate complex relationships with different private sector entities located in different jurisdictions. Stakeholders cited significant differences in the quality of relationships between certain private sector companies (particularly larger social media or communications platforms) and different European countries, particularly those states with a smaller intelligence and law-enforcement presence, or a less long-standing terrorism problem. These challenges directly affected operational outcomes and contributed in turn to a greater reliance on intelligence from overseas services (in some national contexts).
- **Technology developments and "going dark"**: the evolution in the capabilities offered by a range of new technologies, including drones, digital forensics and AI, and the extent to which most aspects of our lives are online in some way, are offering government actors new capabilities to better monitor and understand the activities of terrorist actors. However, these and other new technologies are also presenting new challenges to this monitoring, notably through the widespread use of encryption. Where this latter issue had previously primarily affected the ability of law-enforcement and intelligence agencies to intercept terrorist communication activity, it is now increasingly also affecting digital forensics across a much wider range of devices (including drones, cars and Internet of Things devices). This meant that government actors risked losing sight of the misuse of a much wider range of new technologies and any associated insights into future potential risks.
- **Incoherent strategic objectives**: despite several decades of evidence to the contrary, counter-terrorism rhetoric continued to include references to preventing any misuse of a particular technology by terrorists, with this rhetoric sometimes affecting the strategic aims of relevant activities (for example legislation relating to the removal of terrorist content from online services). Some interviewees felt that an inability to recognise that complete prevention was essentially impossible was inhibiting an adjustment to the overarching aims of responses, and the specific activities underneath them.

- **Siloed, CT-specific approaches**: although well-established (and broadly successful) terrorism-specific responses have been developed, particularly in the context of terrorist content online and terrorist financing, interviewees felt that insufficient attention was given the connectivity between these responses (and the phenomena they were responding to) and broader policy areas and context. Despite counter-terrorism not always being the most appropriate lens to approach challenges through (or at least not the only lens), it still tended to predominate.
- **Human rights risks**: although new technology offers significant potential to improve or enhance a range of counter-terrorism efforts, these powerful tools also bring with them significant human rights risks, particularly in relation to the legitimate activities of civil society and human rights groups. In some instances, human rights abuses were occurring due to the overreach of government actors, whether deliberately or accidentally, but they also occurred due to the actions of private sector entities, either in response to government requests or due to the overzealous misapplication of terms of service.
- **Conflict between privacy and security**: interviewees also raised concerns about the prevalence of overlapping or conflicting legislation, particularly with regard to levying security requirements that might be at odds with privacy requirements. This conflict was of particular concern for private sector companies seeking to navigate the legislative requirements. Simultaneously, some government interviewees still felt that the balance between these two principles tipped too heavily in favour of privacy, limiting the technical capabilities at their disposal, particularly with regard to interception and encryption.
- **Geopolitical context**: several interviewees mentioned the challenges associated with a fraying international order in which multilateralism faced numerous challenges and national and regional competition had increased. As a result, there was a growing divide in terms of human rights standards, approaches to new technologies and even the governance of the internet itself, with technology seen as a vector for competition, not co-operation. This posed growing challenges for many stakeholders, notably tech companies, many of whom were transnational or international in nature. As a result, they found themselves having to juggle different national or regional legislative requirements and standards, which were often in conflict with each other.

Good practices

- **Horizon scanning**: some interviewees observed that by conducting horizon scanning or strategic foresight exercises, their organisations had successfully reduced the time lag between terrorist misuse of new technology occurring and the associated risks being identified. By identifying these risks more quickly, organisations across multiple sectors were becoming better placed to respond to them.
- **Multistakeholder approaches**: to help facilitate these kinds of exchanges, stakeholders emphasised the effectiveness of multistakeholder forums, which had already delivered better information sharing between national governments and private sector companies. Although this type of approach came with significant challenges, including issues of trust, security and resources, it was seen as critical to better understanding each sector's approaches and insights, and had helped to create a meaningful feedback loop between all of the different entities involved. One example of this approach in the context of threat and risk identification was GIFCT's use of multistakeholder working groups to conduct "red team" exercises on emerging threats, including 3D-printed weapons.[105] Operationally, Europol's European Platform for Removing Illegal Content Online (PERCI) system had also allowed EU member states to standardise their referral of terrorist content to private sector entities and receive valuable feedback to improve future co-operation.
- **Trends identification role of academia and civil society**: although state or private sector actors typically have access to classified or sensitive material that provides them with a unique insight into emerging trends, interviewees also highlighted the vital role that academic or civil society institutions were playing in supplementing these sources. Examples cited included the research conducted by the GIFCT-supported Global Network on Extremism and Technology (GNET),[106] and the activities of Europol's European Counter Terrorism Centre (ECTC) Advisory Network.[107] This research (and that produced by a range of other research networks and institutions) was critical for, and widely used by, private sector

105. GIFCT Red Team Working Group, "Risks and challenges in online communities for 3D-printed firearms among extremists and terrorists", 20 September 2023.
106. See the GNET website for more information.
107. See Europol's website for information about the Advisory Network's 2024 annual conference.

companies facing challenges with the misuse of the platforms or technologies by terrorist actors. Civil society actors were also often well-placed to identify emerging harms, given their connections to the communities most affected by terrorism and violent extremism.

- **Private sector collaboration**: stakeholders felt that private sector companies also needed forums within which they could share lessons learned regarding how terrorists were exploiting their technology and how best to respond. Good practices established in the context of terrorist use of the internet and terrorist financing could be used as a model to be followed in other technological contexts, although it was recognised that greater efforts were required to bring in a more diverse range of companies. In particular, greater support was required for smaller companies, which typically had less resources to respond directly to terrorist misuse, address law-enforcement requests and understand legislative or regulatory requirements, often across multiple jurisdictions. In addition to the sharing of information and good practices, this collaboration could also come in the form of peer-to-peer mentorship and training or support.
- **Clear strategic objectives**: strategic objectives (and their associated language) were more effective when they focused on what was achievable – which was defined as making it as difficult as possible for terrorists to misuse a given technology – rather than on what sounded powerful rhetorically. Having this type of strategic objective typically resulted in approaches that focused on creating barriers to entry for terrorist use of a given technology and limiting the reach and impact of their related activity. Stakeholders felt this approach could still make a positive impact on the terrorist landscape.
- **Technology-neutral approaches**: interviewees contrasted the effectiveness of technologically neutral approaches that focus on the desired outcomes, versus those that attempted to spell out the steps required to achieve them. The latter approach – particularly when focused on tech-driven activities – risked legislation becoming obsolete or outdated as the threat and response landscape evolved in response to new technologies. When the former approach was taken, private sector companies were able to utilise their expertise to deliver a greater impact.
- **Better use of existing tools and approaches**: some interviewees commended responses to terrorist exploitation of new technologies that included the leveraging of tools and legislation that had been developed in different counter-terrorism contexts. For example, individuals supplying UAS or other new technologies to terrorist actors could be subject to sanctions under the obligations of United Nations Security Council Resolutions 1267 (1999) and 1373 (2001).
- **Broader approaches that better integrate with/connect to non-counter-terrorism responses**: stakeholders felt that effective counter-terrorism responses, particularly in the context of technology, were those that were better connected to a broader policy environment. They typically also recognised when there were parts of the terrorism and new technology problem that were better addressed in a non-counter-terrorism context.

Conclusions

Building on the findings of the report, particularly the insights gained during the interview process, the following section provides a limited set of recommendations for Council of Europe member states, other government agencies, intergovernmental institutions, private sector actors and civil society.

- **Counter-terrorism and P/CVE actors should seek to identify and evaluate new technology-related risks more quickly**. Shortening the time lag between terrorist experimentation occurring and its identification can allow counter-terrorism actors to better contextualise the potential risks a technology might pose, which may in some cases be less significant than previously thought, and improve how quickly responses can be developed (where required). This can be achieved through an ongoing horizon scanning function or ad hoc strategic foresight exercises such as red teaming. Greater engagement with (and between) stakeholders from different sectors can also contribute to this identification and response process.
- This should be complemented by efforts to **improve information sharing related to the exploitation of new technology by terrorists**. Although information sharing is a perennial, long-standing counter-terrorism challenge given sensitivities relating to capabilities and operational activities, sharing anonymised or disaggregated data related to terrorist misuse and exploitation of new technology (for example trends related to the misuse of AI) can result in an improved, collective understanding of the risks it may pose. Where possible, sharing should take place not only within and between national authorities and with regional and international partners, but also between governments, the private sector, civil society and academia, helping to address variance in capabilities, relationships and information access, and the transnational nature of the current terrorist landscape.
- Each of these recommendations points towards the importance of **developing multistakeholder approaches to the exploitation of new technologies by terrorist actors**. In addition to information sharing, this should include meaningful dialogue, creating forums for sharing lessons learned and good practices, opportunities for mentorship and capacity-building support (including the provision of specific tools and techniques), and the creation of feedback loops to help shape and iterate responses.
- These approaches should also seek to involve less traditional partners, including entities with experience in responding to new technology-related threats in other contexts, helping to develop a **more holistic, less siloed approach to the exploitation of new technology**. By learning from the experiences of a broader range of organisations, counter-terrorism actors can integrate new approaches or new partners within their responses.
- **Greater efforts are needed to manage and mitigate the significant human rights risks** that are often associated with the tools and approaches used to counter terrorist use of new technologies. Many of the above recommendations should assist in this regard, particularly the greater inclusion of civil society. However, these should be complemented by robust transparency and oversight mechanisms (for public and private sector organisations) and regular feedback from human rights organisations.
- Counter-terrorism actors should also **strive for greater clarity when articulating their objectives, including by considering technology-neutral approaches**. By focusing on creating barriers to entry for terrorist use of a given technology or limiting the reach and impact of their related activity, counter-terrorism actors are more likely to achieve a positive impact on the terrorist landscape. This clarity of focus may also result in the creation of technology-neutral approaches, allowing the private sector and other stakeholders to remain focused on the desired outcome, particularly in light of rapid changes to the technological landscape.

For over 40 years, the Council of Europe has worked to develop and reinforce key legal standards to prevent and suppress acts of terrorism. By taking a comprehensive approach, the Organisation helps member states fight terrorism more effectively by strengthening and improving their national legislation, thereby facilitating international co-operation. With full respect for human rights and the rule of law, the Council of Europe is continuously striving to bring terrorists to justice and bolster international co-operation.

PREMS 082125

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE