The Terrorism Acts in 2021

REPORT OF THE INDEPENDENT REVIEWER OF TERRORISM LEGISLATION ON THE OPERATION OF THE TERRORISM ACTS 2000 AND 2006, AND THE TERRORISM PREVENTION AND INVESTIGATION MEASURES ACT 2011

By JONATHAN HALL K.C.

Independent Reviewer of Terrorism Legislation

March 2023

The Terrorism Acts in 2021

REPORT OF THE INDEPENDENT REVIEWER OF TERRORISM LEGISLATION ON THE OPERATION OF THE TERRORISM ACTS 2000 AND 2006, AND THE TERRORISM PREVENTION AND INVESTIGATION MEASURES ACT 2011

By JONATHAN HALL K.C.

Independent Reviewer of Terrorism Legislation

Presented to Parliament pursuant to Section 36(5) of the Terrorism Act 2006

March 2023

© Crown copyright 2023

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at:

Direct Communications Unit
Home Office
2 Marsham Street
London
SW1P 4DF

ISBN 978-1-5286-3961-3

E02876111 03/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

INDEX

EXECUTIVE SUMMARY

- The internet is the new frontier for counter-terrorism.

- This annual report on the operation of the Terrorism Acts during 2021 seeks to describe UK and international machinery for countering terrorist content online and reviews the application of UK terrorism legislation in the online context.

- It asks and tries to answer: What is online radicalisation? How relevant are terrorist organisations? What values and standards should guide online counter-terrorism? Who is a "member of the public" online?

- The internet has provided new opportunities to investigate suspected terrorism by picking through masses of online data but this requires new safeguards in context of remote access, retention and deletion, and biometrics.

- Online content is drawing more and more children into the terrorism and counter-terrorism sphere. I consider diversionary options but also look critically at whether the modern slavery defence does (and ought to) apply for children where terrorist prosecution is required.

- Online terrorism requires a new approach to the assessment of terrorist risk. There are more individuals with poor mental health or neurodivergence whose risk and needs must be managed, even in the context of serious and sophisticated counter-terrorism measures like TPIMs.

- Tech companies are central to the use of the internet to commit terrorism offences and to the presence of terrorism content in our lives. The report examines the means available in the UK to encourage or mandate content moderation by tech companies. I question why the Online Safety Bill excludes terrorism content from heightened child-specific duties.

- This report makes 8 recommendations.

1. INTRODUCTION

1.1. This is my fourth annual report on the operation of terrorism legislation in the UK, and it comes with a specifically online perspective.

1.2. Terrorism legislation in the UK is largely the product of laws designed to detect and inhibit organised terrorist groups in Northern Ireland. 20 years after dial-up modems and the enactment of the Terrorism Act 2000 is a good time to report on whether terrorism laws still measure up.

1.3. Alongside the assessment of legislation, I have attempted to describe how online counter-terrorism operates in the real world and sought to answer some questions which are easy to ask but difficult to answer. So much depends on the role of tech companies, and comparatively less on the role of law enforcement and public bodies.

1.4. Terrorism laws contains relatively little express reference to online activity or content. Aside from additions to sections 13 (displaying articles associated with proscribed groups) and 58 (streaming of information useful to terrorists) Terrorism Act 2000[1], the key provisions are found in the Terrorism Act 2006[2].

1.5. The 2006 Act created the offences of encouraging terrorism, and disseminating terrorist publications, and made them directly applicable to defendants who used electronic systems to make terrorist content accessible to the public. As I discuss in Chapter 7, the commission of these terrorism offences is so easy that it is increasingly difficult to distinguish between terrorists (who deserve the full attention of counter-terrorism police) and those whose actions may be criminal but fall below the threshold at which national security is engaged.

1.6. It is true that embedded within the Terrorism Act 2000's definition of terrorism is a type of terrorist action that would neatly fit a terrorist cyberattack, and there are cases of successful cyber attacks carried out by terrorists or hackers aligned to proscribed organisations[3]. But only one person has to date been prosecuted in the UK for an

[1] As amended by the Counter-Terrorism and Border Security Act 2019.
[2] Sections 1-3, 20.
[3] https://www.hackread.com/hezbollah-hackers-global-malware-attack/ (last accessed 7.1.23).

attack "…designed seriously to interfere with or seriously to disrupt an electronic system"[4], and that related to a physical plot to damage transmitter masts[5].

1.7. The fact that terrorists use the internet is obvious and I have not sought to describe how they do so. Trying to list all the ways in which terrorists and their sympathisers use an ever-evolving medium would be a heroically impossible endeavour, and there is a wide body of academic literature devoted to cataloguing examples[6].

1.8. Suffice it to say that:

- Terrorists have shown themselves to be agile and savvy tech performers[7]**,** early adopters at exploiting all the different uses (termed 'affordances') to which online platforms lend themselves[8].

- They are alert to endeavours to remove content or shut down channels, resulting in a frequent exodus from larger to smaller platforms[9]. Techniques used include content masking, text distortion, disingenuous translations, and hashtag and account hi-jacking[10].

- The rate at which the Christchurch attack video was uploaded in the immediate aftermath, including in files that had been deliberately altered to frustrate blocking technologies[11], suggest that there are tens if not hundreds of thousands of individuals who – for free speech, shock-value, or more sinister motives – are determined to keep such material in circulation.

- Terrorist violence may be enabled through plans formulated (acquiring details of targets) discussed (within a terrorist group or cell) or methods (techniques

[4] Section 1(2)(e) Terrorism Act 2000.
[5] Oliver Lewin, convicted of section 5 attack-planning on 19.12.22.
[6] E.g. Macdonald, S., Rees, C., S., J., 'Remove, Impede, Disrupt, Redirect: Understanding and Combating Pro-Islamic State Use of File-Sharing Platforms' (Resolve Network, April 2022).
[7] Rasmussnen, N., GIFCT Executive Director, 'The Dynamic Terrorism Landscape and What it Means for America' (written testimony to US House of Representatives Commission on Homeland Security, 2.2.22).
[8] For an accessible history of evolving use of platforms between 2003-2019, see Williams, H., Evans, A., Ryan, J., Mueller, E., Downing, B., 'The Online Extremist Ecosystem' (Rand Corporation, December 2021).
[9] HM Government, 'Impact Assessment Online Safety Bill' (311.22) at para 357.
[10] Pool Re, 'Cyber Terrorism: Islamic State's effective exploitation of social media' (27.4.22).
[11] New Zealand Government, '2021: Digital Violent Extremism Transparency Report' (2022), p31.

for killing through to 3-D printed weapons[12]) or materials (components for making explosive devices) obtained on the internet. There are sufficient cases of improvised explosive devices being made to an internet recipe[13] to know that some online material lowers the bar to terrorist acts which were previously dependent on expert bomb-makers or the covert circulation of physical manuals. Explosives manuals are not, however, self-executing. An individual must decide to exploit the know-how for terrorist ends.

- The internet is an effective means of persuasion or radicalisation, whether through points of ideology or cruder forms of inspiration[14].

- The internet is a mechanism for amplifying the effect of violence, or as has long been the objective of terrorists, building antagonism and dividing society[15].

1.9. Two themes running through this review are online conduct and online content.

1.10. Online conduct describes activity conducted via the internet that leads to individuals being investigated, disrupted, arrested, examined at ports, prosecuted, or made subject to special civil measures. Alongside the perils of online terrorism there is the risk of overreach: of children being prosecuted for terrorist offending who lack terrorist intent or capability; or of Counter-Terrorism Police ('CT Police') having access to a surfeit of data held locally or remotely without adequate safeguards on access and retention.

1.11. Online conduct is the focus of Chapters 3 to 8. As before there are separate chapters for Northern Ireland (Chapter 9) and Scotland (Chapter 10), written as far as possible from an online perspective.

1.12. Online content is different. Terrorism legislation is directed against human conduct not against content. Content is not a crime, and content is not itself violent.

[12] R v Hall, Salmon, Wright and Whibley (Doncaster Crown Court, 2022). Basra, R., 'The Future is Now: the Use of 3-D Printed Guns by Extremists and Terrorists', GNET (23.6.22).
[13] Gill, P., Corner, E., McKee, A., Hitchen, P., Betley, P., 'What Do Closed Source Data Tell Us About Lone Actor Terrorist Behavior? A Research Note' (2022) 34 Terrorism and Political Violence 113: evidence of bomb-making manuals was identified in over 70% of their sample.
[14] See Chapter 11.
[15] Burleigh, M., 'Blood and Rage: A Cultural History of Terrorism' (Harper, 2009).

But it is almost impossible to discuss online terrorism without conceptualising content – electronically transmitted and assembled words, images, and sounds – as a third actor interposed between perpetrator and victim, playing an ineffable role in the evolving threat landscape. Causing problems that are directed against living threats, manifestos and videos deposited online by terrorists continues to have persuasive force well after the death of their author.

1.13. Chapter 11 considers terrorism content, and the role that content has in online radicalisation. I also consider the fundamental rights or values that must be considered when devising schemes for removing content in the name of counter-terrorism. Remoteness of words from violence is what makes the topic of radicalisation so difficult.

1.14. Chapter 12 describes the counter-terrorism role played by tech companies and examines how UK legislation may influence how tech companies operate. Recommendations are listed in Chapter 13, together with the government's responses to recommendations made in previous reports.

2. REVIEW OF 2021

The Online Counter-Terrorism Machinery

United Nations

2.1. In 2005, the United Nations Security Council passed Resolution 1624 which required states to act against incitement to terrorism. It referred to the exploitation of sophisticated technology, communications, and resources to incite support for criminal and terrorist acts.

2.2. The word 'internet' first appeared in a counter-terrorism context in UNSCR 1963 (2010): the United Nations expressed concern that the internet was increasingly being used by terrorists for recruitment, incitement, financing, planning and preparation of terrorist activities.

2.3. After 2010, prompted by Islamic State's slick social media operations, the United Nations exhorted states, either directly or in collaboration with the Global Internet Forum for Countering Terrorism[16], to take action to address the "evolving nexus" between terrorism and the internet with an "increased use" by "terrorists and their supporters" (UNSCR 2129 (2013)).

2.4. Separately, the UN drew attention to the need for action in the form of criminalisation, provision of investigative powers, regulation of internet services, more international cooperation, special judicial and evidential procedures, whilst maintaining international human rights standards[17].

2.5. In 2014 the Security Council signalled its readiness to sanction those "associated with Al Qaeda through information and communications technologies including the internet and social media" (UNSCR 2170 (2014))[18], and drew particular attention to the role of the internet in the travel of foreign terrorist fighters (UNSCR 2178 (2014).

[16] See further, Chapter 12.
[17] UN Office on Drugs and Crime, 'The use of the Internet for terrorism purposes' (2012) at para 74. The use of the internet to gather data and investigate was noted in UNSCR 2322 (2016).
[18] Including those who provided Internet hosting and related services: UNSCR 2253 (2015).

2.6. As the 2010s progressed, the UN drew attention to 2 additional aspects:

- Firstly, given the effectiveness of terrorist propaganda, the desirability of creating effective counter-narratives (UNSCR 2253 (2015)), an aspiration that has remained unachieved.
- Secondly, the need to cooperate with civil society and, crucially, given the lack of state control over the internet, the private sector (UNSCR 2395 (2017)).

2.7. UNSCR 2354 (2017) consolidated the UN's focus on "terrorist narratives". These narratives could be used for recruiting supporters and foreign terrorist fighters, to mobilize resources and to garner support from sympathisers. In effect the UN recognised that narratives existing online but not directly targeted at any individual could lead to increased terrorist support: an appreciation of the autonomous role of online content.

2.8. The United Nations Counter-Terrorism Committee Executive Directorate (CTED) formalised its collaboration with the private sector in this area in 2017 under the initiative 'Tech Against Terrorism'[19]. CTED also joined in the work of an industry endeavour founded in 2017, the Global Internet Forum to Counter Terrorism (GIFCT), which was formed after UK pressure following the Westminster attack in March 2017[20]. In 2017, UNSCRs 2395 and 2396 referred to the role of Tech Against Terrorism and GIFCT. I consider the role of these membership organisations in Chapter 12.

2.9. The 2019 terrorist attack in New Zealand, led to the Christchurch Call and a G20 statement[21], both noted in UNSCR 2617 (2021).

2.10. CTED's 2021 global survey of the implementation of UNSCR 1624 (2005) identified a notable increase in online communications aimed at inciting terrorism and violent extremism; and identified a three-fold increase over the previous 5 years in attacks, mostly in Western States, of attacks conducted by individuals affiliated with

[19] UN CTED, 'Information and Communications Technologies', factsheet (May 2021).
[20] HM Government, 'Contest 3.0' (2018) at page 35.
[21] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism.

such movements and narratives[22]. It called for yet more cooperation between the public and private sector.

2.11. In the global South, the UN (through the UN Development Programme) has become involved in some of the consequences of rapid digital growth amongst a young and undereducated population: for example, in Bangladesh following the Holy Bakery attacks in 2016[23] and in Sri Lanka, where anti-Muslim calls for violence spread unfiltered on mainstream platforms[24].

- In both cases there was a lack of language capabilities on the part of giant tech companies, leading to an inability to moderate dangerous content. The role of civil society as trusted flaggers and a point of pressure on tech companies is all the greater where the democratic standards of particular governments are open to question.

European Union

2.12. The EU enacted Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. The principal body is a part of Europol called EU Internet Referral Unit (EU IRU) which has, like the UK's CT Internet Referral Unit, a liaison function between governments and tech companies[25].

2.13. The EU IRU coordinates joints Referral Action Days, in which the UK still participates, to target particular forms of content by identifying it to tech companies for removal in accordance with their own standards[26].

2.14. The EU's Digital Services Act, due to come into force in January 2024, will be to impose harmonised obligations on tech companies providing content within the EU to respond rapidly to the identification by law enforcement of illegal, including illegal terrorist, content.

[22] UN CTED, 'Global survey of the implementation of Security Council resolution 1624 (2005)' (2021), at para 13.
[23] UNDP, 'From preventing violent extremism to building digital citizenship' (17.10.21).
[24] UNDP, 'Promoting Non-Violent Communication and Responsible Use of Media' (14.1.21).
[25] Europol, 'European Union Terrorism Situation and Trend Report 2022', at page 89.
[26] For example, Europol, 'Terrorism and extremist chants used to woo recruits – focus of latest Europol Referral Action Day' (20.5.22).

- The EU has this advantage: it can establish harmonised regulations applying to tech companies who service almost 450 million users. To that extent, it may reduce the burden on tech companies of forced compliance with varying regimes established by individual countries.

- It remains to be seen how EU internet regulation develops further. The amount of terrorism content online means that wide-ranging removal is ultimately dependent on large tech companies and their automated systems: and to that extent any ratcheting up of legal obligation involves an outsourcing of counter-terrorism standards to private companies. But even small platforms, with limited assets and employees (let alone legal departments) may quickly establish huge reach and be exploited by terrorists: these may be unlikely to be able to respond to obligations, stump up registration fees, or pay fines.

UK Strategy

2.15. The UK's CT strategy is known as 'Contest'. The 2011 version noted the internet's transformative effect on the operation of terrorist organisations but made the assumption that over the next 4 years the internet would rarely be a substitute for the "social process of radicalisation"[27]. With the benefit of hindsight this assumption underplayed the extent to which lone individuals would be drawn into terrorist offending by the internet; although, as discussed in Chapter 5, there remains legitimate doubt about the degree of risk posed by lone self-radicalised individuals, compared to those who are part of or associate themselves with traditional terrorist organisations.

2.16. The next (and current) edition of Contest in 2018 observed that the internet was now firmly established as a key medium for propaganda, radicalisation and attack preparation[28] and noted that more internet-connected devices, stronger encryption and cryptocurrencies, plus the dispersal and anonymity of data, could frustrate counter-terrorism operations[29].

2.17. In its Integrated Defence Review of 2021, the government set out the ambitious objective of ensuring that there are "no safe spaces online in which terrorists can

[27] HM Government, 'Contest' (2011) at pages 73, 41.
[28] HM Government, 'Contest 3.0' (2018) at para 78.
[29] At para 79.

promote or share their extreme views", emphasizing the importance of collaboration with tech companies, international partners and civil society organisations[30].

2.18. In 2021, under UK chairmanship, G7 leaders issued a statement on online violent extremism and terrorism[31]: here the emphasis was on the tech industry, and the limitations on what governments could achieve.

Home Office

2.19. The Homeland Security Group within the Home Office contains an Internet Policy Unit. This unit:

- leads on government policy for 'Preventing Terrorist Use of the Internet'.
- Engages with tech companies, the GIFCT and international partners.
- has responsibility for the terrorism aspects of the Online Safety Bill (led by the Department for Digital Culture Media and Sport, DCMS[32]).

2.20. Other parts of the Homeland Security Group are responsible for investigative powers relevant to online counter-terrorism such as encryption or remote data.

2.21. The Research, Information and Communications Unit (RICU) is a government strategic communications unit [33] which among other things analyses terrorist propaganda. It works with the Extremism Analysis Unit, also part of the Home Office[34].

UK Police

2.22. The nature of online terrorism is that its perpetrators may be sitting at a screen anywhere in the world. In the UK, CT Police have needed to carry out arrests in areas that traditionally had little or no counter-terrorism footprint.

[30] HM Government, 'Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy' (2021), at page 81.
[31] 'G7 Statement on Preventing and Countering Violent Extremism and Terrorism Online' (2021).
[32] DCMS also has responsibility for general internet infrastructure and governance.
[33] HM Government, Response to 8th report from Home Affairs Select Committee Session 2016-17, Cm 9555 (2017).
[34] Intelligence and Security Committee (ISC), 'Extreme Right Wing Terrorism', HC 459 (13.7.22), at para 137.

2.23. Stepping out of the shadows, CT Police have openly called for vigilance, especially from parents towards their children[35] and for alerts of terrorist content online (via a Home Office reporting portal[36]). In the summer of 2022, the police were reported to have sent out letter to schools warning of online radicalisation[37].

2.24. CT Police also have a role in the Prevent process[38]. At the time of writing, the independent review into Prevent by William Shawcross CVO has been delivered to the government but not yet published.

2.25. The National Digital Exploitation Service (NDES) is a specialist part of CT Police which was set up in 2016[39]. It deals with technical aspects of interrogating and securing electronic data.

2.26. NDES now hosts the CT Internet Referral Unit, which was established in 2010. Among other things CTIRU receives public reports about online terrorism for investigation. Some content may be referred to tech companies to consider removal based on their policies and terms and conditions. By 2021, 318,966 items of content had been voluntarily removed by tech companies since 2010 because of CTIRU intervention[40].

2.27. The relationship between CTIRU and tech companies is a brokered one, based on trust, experience and individual relationships and the responsiveness of different tech companies differs massively. The willingness of individual companies to engage with CTIRU can be measured in practical matters such as whether they are willing to provide a phone number, or whether they insist that all contact is done, of whatever sort, on their terms via an internet portal or email address.

2.28. As discussed in Chapter 12, CTIRU have never used the power under section 3 Terrorism Act 2006 to require content removal. The most likely explanation, aside from the complexity of the legislation, is the limits of enforcement: CT Police recognise

[35] During 2021 Counter Terrorism Policing released 54 news items on their website (www.counterterrorism.police.uk). In 10 of these, the police drew attention to the risk posed to children by online terrorism content and asked for vigilance.
[36] https://www.met.police.uk/tua/tell-us-about/ath/possible-terrorist-activity/report-online-terrorist-activity/?tid=2125&lid=&cid=&rid=5&stepid=1 (last accessed 3.10.22).
[37] 'Children could be radicalised over summer break, Met Police warn parents', Observer (24.7.22).
[38] HM Government, 'Channel Duty Guidance' (2020).
[39] 'Contest 3.0', supra, at para 151.
[40] HM Government, 'Transparency Report: Disruptive Powers 2020' (2022) CP 621.

that persuasion is their only effective tool for the mainly overseas websites with which they deal.

2.29. As tech companies have become more proactive, referrals by CTIRU have decreased somewhat[41].

UK Intelligence Agencies

2.30. MI5 and GCHQ play a critical role in identifying online terrorism: a role that since 2018 has extended to Extreme Right Wing Terrorism alongside Islamist and Northern Ireland-Related Terrorism[42]. Engagement with overseas agencies is also key.

2.31. At the sharper end, GCHQ and the Ministry of Defence have used cyber capabilities against Islamic State/Da'esh communications and propaganda functions[43].

Events

Domestic

2.32. There were two completed attacks in 2021 in Great Britain.

2.33. In October 2021, Ali Harbi Ali murdered Sir David Amess MP at his constituency surgery.

- This Islamist terrorist attack was carried out with a knife following months of surveillance of potential targets including other Members of Parliament.
- He was convicted of murder and preparation of terrorist acts[44] and sentenced to a whole life term of imprisonment.
- The sentencing remarks reveal that he was radicalised over the internet in early adulthood to become a supporter of Islamic State/ Da'esh[45].

[41] CT Policing, 'Together, we're tackling online terrorism' (19.12.18).
[42] ISC, *supra*, at paras 238-9.
[43] HM Government, 'National Cyber Strategy 2022' at page 110.
[44] Section 5 Terrorism Act 2006.
[45] Sweeney J. (13.4.22), at para 4.

- Unwilling or unable to travel abroad to carry out physical jihad, Ali heeded online calls from Islamic State spokesmen to carry out an attack at home. He purchased the knife used in the attack in 2017[46].
- Ali used the internet to obtain targeting information for an attack on Michael Gove MP, Sir David Amess MP, and Mike Freer MP, and then carried out physical hostile reconnaissance[47].
- Ali then sent deceptive emails to Sir David's office, pretending to be a constituent and arranging to come for the constituency surgery, where he carried out his attack[48].

2.34. In November 2021, Emad Al Swealmeen was killed when his own bomb went off in a taxi outside Liverpool Women's Hospital on Remembrance Sunday. The taxi driver was injured but not killed.

- CT Police declared the incident to be a terrorist attack and carried out three arrests under the Terrorism Act (the suspects were all released with no further action).
- An inquest heard that Al Swealmeen turned a rented flat into a "bomb-making factory" and called his brother 2 days before the attack to suggest he was going to do "something bad" [49].
- CT Police have not revealed whether Al Swealmeen, a practising Muslim who faked a conversion to Christianity and was assessed under the Mental Health Act 1983 in 2015, was influenced by Islamist ideology. The attack was similar in methodology to recent Islamist terrorist attacks.
- The inquest did not determine motivation other than to find that Al Swealmeen acted "with murderous intent"[50].

2.35. A result of these two attacks was that on 15 November 2021 the government increased the threat level from SUBSTANTIAL to SEVERE[51] where it remained until February 2022.

[46] Ibid, paras 5-7.
[47] Ibid, paras 8-11.
[48] Ibid, paras 14-17.
[49] 'Liverpool bomber made device with murderous intent, coroner says' (BBC News, 30.12.21).
[50] Ibid.
[51] Home Office announcement, 'UK terrorism threat level raised to SEVERE' (15.11.21).

2.36. In 2021 there were 4 late-stage plot disruptions[52], compared to a total of 31 between 2017 and September 2021[53]. None of the 4 late-stage plots in 2021 was Islamist[54].

2.37. The fatal gun attack in Plymouth in August 2021, in which Jake Davison killed 5 people, injured 2 others, and then shot himself was not considered to be a terrorist attack.

- The attack is a reminder that the availability of firearms may be the most important difference between alarming rate of internet-inspired shootings in the United States, and the generally low figure for terrorist deaths in the UK. It led to a review of firearms licencing in England and Wales.
- Davison had been reported to Prevent in 2016 and is reported to have been drawn to incel ideology. An inquest is due to take place in 2023.
- I considered incels and terrorism in a previous report. In short, inceldom is capable of being a terrorist ideology, but whether to treat a particular attack as a terrorist attack is fact-specific and depends in part on the wider security context[55].

2.38. I refer to terrorist attacks in Northern Ireland in Chapter 9.

2.39. The Director General of MI5 revealed in a speech in July 2021 that Extreme Right Wing Terrorism (ERWT)[56] was the subject of one in five CT investigations, and that an even higher percentage of recent disrupted late-stage attack plots had been ERWT. However, the ERWT threat had some challenging characteristics:

- The high prevalence of children.
- Obsessive interest in weaponry, presenting difficult choices where it was not clear that the interest in weapons was linked to any terrorist intent.
- "And always, always, the online environment"[57].

[52] 'Terrorism: Children with extreme right-wing ideologies 'getting substantially younger' as 19 arrested' (Independent, 17.3.22).
[53] Set against: 'MI5: 31 late-stage terror plots foiled in four years in the UK' (BBC News, 1.9.21).
[54] Source: NCTPHQ. Whereas the total 31 plots were "largely Islamist": ibid.
[55] Terrorism Acts in 2019 at 2.28 et seq.
[56] The renaming of Right Wing Terrorism as Extreme Right Wing Terrorism, following a complex cross-Whitehall review of over 40 options, was endorsed in the ISC's report, supra, at para 21. This suggests that if left wing or animal rights or environmental terrorism rears its head, the government will need to consider an addition to those nomenclatures.
[57] MI5, 'Director General Ken McCallum gives annual threat update 2021' (14.7.21).

2.40. There were no successful ERWT attacks in 2021. I consider the focus of CT activity on children, and the nature of the link between online content and terrorist violence throughout this report.

2.41. In February 2021, the Supreme Court handed down its judgment in the case of Shamima Begum[58], an interim ruling in her as yet-undetermined challenge to the decision of the Home Secretary to deprive her of her British citizenship in 2019[59].

- Of importance to legislation such as the TPIM Act 2011 and the Counter-Terrorism and Security Act 2015[60] that require the Secretary of State to assess terrorist risk and its appropriate mitigation, is the Supreme Court's restatement of the role of judicial review and appellate courts.

- Where a case concerned "…an evaluative judgment of matters, such as the level and nature of the risk posed by the appellant, the effectiveness of the means available to address it, and the acceptability or otherwise of the consequent danger, which are incapable of objectively verifiable assessment", the Secretary of State's assessment had to be accorded appropriate respect, for reasons both of "institutional capacity" and "democratic accountability"[61].

- The Supreme Court overturned the decision of the Court of Appeal to allow Begum to re-enter the UK.

- The government may feel that the Begum judgment reduces some of the litigation risk it faces in challenges to national security matters. It remains to be seen whether this feeds through into decision-making.

International

2.42. The EU has reported a total of 15 completed, foiled, and failed terrorist attacks in 2021, although any international statistics come with the caveat that there is no

[58] R (on the application of Begum) v Special Immigration Appeals Commission [2021] UKSC 7.
[59] Under section 40 British National Act 1981.
[60] Temporary Exclusions Orders. TPIMs and TEOs are considered in Chapter 8.
[61] At para 70.

internationally agreed definition of terrorism, and different states may record attacks or plots differently.

2.43. According to this report, France experienced the highest number of attacks (5), followed by Germany (3) and Sweden (2). Austria, Denmark, Hungary, Belgium, and Spain reported one attack each. Of the 15 attacks, 11 were reported as jihadi terrorism.

- The four completed attacks comprised three jihadist terrorist attacks and one left- wing terrorist attack.
- Two of the three completed jihadist attacks in France and Spain caused a total of two deaths.
- The 2021 total of completed, foiled, and failed attacks is considerably lower than in the previous year (57). This is said to be due to a significant decrease in the number of attacks reported as left-wing terrorism[62].

2.44. Europol's analysis of jihadist propaganda in 2021[63] established that there was a dip in officially produced Islamic State propaganda; Islamic State propaganda was mainly produced by IS-supporting media outlets; France, the United States and Israel were the focus of AQ online threats; AQ-supporting media drew succour from the withdrawal of Western troops from Afghanistan.

2.45. Worldwide in 2021[64]:

- deaths from terrorism fell by 1.2 per cent to 7,142 deaths and are now a third of what they were at their peak in 2015.
- However, attacks increased from 2020 by 17 per cent to 5,226 in 2021, largely due to violence in the Sahel region and instability in country such as Afghanistan.
- The data shows a shift in the dynamics of terrorism, with terrorism becoming more concentrated in regions and countries suffering from political instability and conflict, such as the Sahel, Afghanistan. Violent

[62] Europol, 'European Union: Terrorism Situation and Trend Report' (2022).
[63] Europol, 'Online Jihadi Propaganda: 2021 in Review' (2022).
[64] Institute for Economics & Peace, 'Global Terrorism Index 2022: Measuring the Impact of Terrorism' (Sydney, March 2022).

conflict remains a primary driver of terrorism, with over 97 per cent of terrorist attacks in 2021 taking place in countries in conflict.

- The Sahel is of serious concern.
- "Politically motivated terrorism" has now overtaken religiously motivated terrorism, with the latter declining (according to the Global Terrorism Index) by 82 per cent in 2021.
- The four terrorist groups responsible for the most deaths in 2021 were Islamic State (IS), Al-Shabaab, the Taliban and Jamaat Nusrat Al-Islam wal Muslimeen (JNIM). These four groups were responsible for 3,364 deaths from terrorism, representing 47 per cent of total deaths in 2021. Another 2,775 of terrorism deaths were not attributed to any organisation[65].

2.46. The unlawful entry of protesters into the United States Capitol building was described by the Director of the Federal Bureau of Investigation as an act of 'domestic terrorism'[66].

2.47. In August 2021 came the military withdrawal of the United States, together with allies including the United Kingdom, from Afghanistan. The Afghan Taleban quickly established control. Although not itself a proscribed organisation under the Terrorism Act 2000, the home affairs portfolio has gone to a key member of the proscribed Haqqani Network[67] and many members of the Taleban are subject to financial sanctions[68].

- Operation Pitting involved the airlift of over 10,000 Afghan nationals to the United Kingdom and would have involved an element of counter-terrorism screening.
- The fear is that Afghanistan will become a safehaven for terrorists looking to attack overseas. The government will undoubtedly face dilemmas in how and whether to seek to influence the unrecognised Taleban government to bear down on the local branch of Islamic State (Islamic State Khorasan Province).

Legislation

[65] Ibid, at p15.
[66] 'FBI chief calls Capitol attack domestic terrorism and rejects Trump's fraud claims' (Guardian, 11.6.21).
[67] Proscribe since 2015.
[68] Under the Afghanistan (Sanctions) (EU Exit) Regulations 2020.

2.48. The Counter-Terrorism and Sentencing Act 2021 established major changes to the sentencing of terrorist offenders, and their management on release, together with changes to the TPIM regime. I referred to these changes throughout last year's annual report. During 2021 the Sentencing Council consulted on changes to their sentencing guidelines required by the uplifting of maximum sentences[69]. Revised guidelines were subsequently published in July 2022.

2.49. The enactment of the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 means that the authorisation of criminal conduct by CHIS is on a more secure statutory footing. More generally, the supporting revised Code of Practice expressly refers to the creation of online presences to investigate terrorism[70].

2.50. 2021 saw various pieces of national security-related legislation with relevance to counter-terrorism:

- Overseas Operations (Service Personnel and Veterans) Act 2021, designed to address liability and investigation of alleged offences in historical overseas operations.
- Authority to Carry Scheme and Civil Penalties Regulations 2021 SI 2021/323; Immigration (Isle of Man) (Amendment) Order 2021 SI 2021/1277; Immigration (Jersey) Order 2021 SI 2021/1281. These provisions are all relevant to border security.
- Counter-Terrorism and Border Security Act 2019 (Commencement No. 1) (Northern Ireland) Regulations 2021 SI 2021/622, which bring into force paragraphs 44 and 45 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019 in relation to Northern Ireland and the retention of biometric data in hostile state cases.

2.51. Broader national security considerations underpinned the Telecommunications (Security) Act 2021 and the National Security and Investment Act 2021.

[69] My response to the consultation is here: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2021/11/2111010-Response-to-Sentencing-Council.pdf.
[70] At para 5.30.

2.52. New Zealand amended its terrorism legislation to enable the investigation and prosecution of preparatory acts[71]. This followed the attack in September 2021 by Ahamed Samsudeen, a known Islamic State supporter injured 8 people in a supermarket in Auckland, New Zealand. He was under armed surveillance at the time, suggesting significant intelligence that he was prepared to carry out a terrorist attack[72].

[71] New Zealand government, 'Counter-Terrorism Legislation Bill passes into law' (30.9.21).
[72] 'Auckland mall terror attack one year on: Questions remain on anniversary' (New Zealand Herald, 3.9.22).

3. TERRORIST GROUPS

3.1. Proscription supplements general terrorism offences by enabling the authorities to act against group-related conduct that falls below the level of general terrorist offending[73].

- For example, it is an offence to raise funds or invite support for a terrorist organisation[74], irrespective of whether the funds will be used for terrorist or non-terrorist purposes (such as paying the heating bill), and whether the call for support is an encouragement to terrorism.
- This allows the authorities to degrade the operational effectiveness of terrorist organisations in a wide range of circumstances.

3.2. Banning terrorist organisations has proven an effective basis for action against groups such as Al-Muhajiroun and National Action[75]. It is a powerful and blunt tool which requires careful handling. Because of the potential impact of proscription, the decision-making process is rightly painstaking[76].

The Role of Groups

3.3. Around the world established groups dominate terrorist killings. According to the Global Terrorism Index, during 2021 47% of terrorist deaths could be attributed to just 4 groups (Islamic State, Al Shabaab, the Taleban, and Jamaat Nusrat Al-Islam wal Muslimeen) [77].

3.4. In the United Kingdom Islamist terrorist groups such as ISIS exercise a pull for lone actors such as Ali Harbi Ali, the killer of Sir David Amess[78], who appear to regard themselves as part of a wider soldiery. Whether it is because these groups have a catalogue of attacks to their name or have exercised territorial control (in Syria and Iraq, in the Horn of Africa, in Afghanistan), or otherwise, they are inspirational and

[73] See further, Terrorism Acts in 2018 at 3.17 et seq.
[74] Section 13 taken together with section 1(5); section 12(1).
[75] Although the problem of proscribed organisations in Northern Ireland is an enduring one.
[76] The Secretary of State acts on the recommendation of the Proscription Review Group, an ad hoc group of cross-Whitehall officials with sometimes differing departmental views on the merits of proscription.
[77] Institute for Economics & Peace, 'Global Terrorism Index 2022: Measuring the Impact of Terrorism' (Sydney, March 2022) at page 15.
[78] Sentencing remark, Sweeney J. (13.4.22).

alignment with these groups points to danger. Present-day terrorism in Northern Ireland remains dominated by offshoots of the IRA.

3.5. The internet provides communication channels for established terrorist groups such as Islamic State to consolidate or grow their traditional group activity. For example, Islamic State sought to swell its physical members by inviting new recruits to travel to Syria/Iraq in the heyday of the so-called Caliphate to fight and support fighters[79].

3.6. For reasons not understood, although possibly for reasons of gun control, or simply because they were caught in time, individuals associated with proscribed Extreme Right Wing Terrorist ('ERWT') groups have not, in the UK, proven as lethal. The terrorist activities of banned right wing terrorist organisations such as Sonnenkrieg, Feuerkrieg, Atomwaffen and the Base are – at least in the UK – predominantly online[80].

- Their activities were illustrated in the case of Andrew Dymock, imprisoned for 7 years in late July 2021: he ran Sonnenkrieg Division and System Resistance Network[81], from his bedrooms in Bath and (as a student) in Aberystwyth, using websites and Twitter accounts[82], calling for a Neo-Nazi race war.

3.7. In its report on Extreme Right Wing Terrorism, the Intelligence and Security Committee of Parliament noted that the number of real-world organised ERWT groups in the UK remains low, although the online space has proven an effective platform to "exert influence and recruit others" [83].

3.8. This is not necessarily recruitment to join a group. Leaderless resistance, to which the internet is so conducive, is a tactic expressly advocated by Atomwaffen and the Base[84], and has a long pedigree[85]. From the group's own perspective, decentralisation is also seen as a counter to law enforcement[86].

[79] Home Office and Department for Education, 'How social media is used to encourage travel to Syria and Iraq' (Briefing note for schools, undated).
[80] Home Office, Proscribed terrorist groups or organisations (updated 26.11.21).
[81] Identified as an alias for National Action, in February 2020.
[82] 'Neo-Nazi Andrew Dymock jailed for terror and hate crimes', BBC News (21.7.21).
[83] 'Extreme Right Wing Terrorism', HC 459 (2022), at para 39.
[84] Ibid; 'Atomwaffen Division', Centre for International Security and Cooperation, Stanford.
[85] Feldman, M., 'Politics, Intellectuals and Faith' (ed. Henderson, A., Columbia, 2020).
[86] Lee, B., 'Think global, act local: Reconfiguring siege culture' (Crest Research, 2021).

3.9. In the early years of the millennium, the argument was made that terrorism legislation (in Great Britain) was essentially anti-Muslim. The UK's proscription of an array of ERWT groups in recent years has had operational benefits (particular for executive steps against National Action) and perceptual ones, although officials are clear with me that there is no intent to 'even up'.

3.10. The UK's proscription of ERWT groups has also been welcomed by tech companies; as I describe in Chapter 12, proscription by a democratic state is a clear and defensible basis for content moderation. I consider below the extent to which proscription under the Terrorism Act 2000 could or should be extended for the purpose of influencing the behaviour of tech companies.

3.11. The boundary-point at which activity by overseas groups crosses into proscription territory is not a clear one. There might come a stage where the tactical advantages of proscription in respect of a transient online group could call into question the use of such a powerful tool, although, having attended each of the Proscription Review Group meetings, I cannot say that it has yet been reached.

Proscription activity in 2021

Atomwaffen Division

3.12. Atomwaffen Division, a mainly US-based white supremacist group which pretended to have disbanded in 2020 but continued to operate under the moniker 'National Socialist Order', was proscribed by the Home Secretary in April 2021[87].

3.13. The explanation for the group's proscription[88] focussed on the threat posed by the group's online promotion of accelerationist violence. It is assessed to have inspired Feuerkrieg Division, already proscribed in the UK in 2020.

3.14. It has been argued that some currently proscribed groups such as Atomwaffen no longer exist in any organisational sense and continue to exist only as a brand[89].

[87] Terrorism Act 2000 (Proscribed Organisations) (Amendment) Order 2021.
[88] Ibid, Explanatory Memorandum.
[89] Jon Lewis, J., Newhouse, A., 'Be Careful Attributing Anything to AWD' (Accelerationism Research Consortium, 04.03.2022).

The Base

3.15. The Base was proscribed in July 2021[90].

3.16. The Base is again a predominantly US-based white supremacist group which advocates accelerationist violence with links to other international groups. The government's explanation pointed to real world 'prepping'-style activity in the US; by implication, the impact in the UK was the group's online presence and advocacy for terrorism[91].

Hamas (Entire Organisation)

3.17. The proscription of the entirety of Hamas was, by contrast, unrelated to online activity. Previously, only Hamas' military wing had been proscribed (from March 2001). In November 2021, both military and political wings were banned[92] with the Home Secretary assessing that the distinction between these wings was artificial and that, as a complex but single terrorist organisation, it committed and prepared for terrorism[93].

3.18. The proscription of Hamas, which governs Gaza, poses the question of how overseas aid agencies can continue to operate in needy parts of the world which are run by terrorist organisations: I consider the position of aid agencies below.

3.19. On the other hand, the fall of the Afghan government to the Taleban in May 2021 did not lead to any Afghanistan-related proscription:

- the group Islamic State Khorasan Province which operates in Afghanistan is no doubt covered by the current proscription of 'Islamic State', without needing to be separately spelt out, in accordance with House of Lords authority on the proscription of the IRA/Real IRA.[94]

[90] The Terrorism Act 2000 (Proscribed Organisations) (Amendment) (No.2) Order 2021
[91] Ibid, Explanatory Memorandum.
[92] The Terrorism Act 2000 (Proscribed Organisations) (Amendment) (No.3) Order 2021.
[93] Ibid, Explanatory Memorandum.
[94] R v Z [2005] UKHL 35. This is the answer to the surprise expressed by the House of Lords Select Committee on International Relations and Defence, 'The UK and Afghanistan' (2019-21 HL 218), para 289, that ISKP was not separately listed.

- The Taleban remains unproscribed even though the home affairs portfolio has gone to a key member of the proscribed Haqqani Network[95] and many members of the Taleban are subject to financial sanctions[96].
- The Taleban undoubtedly meets the threshold for proscription as an organisation concerned in terrorism[97], but in deciding whether to exercise her discretion the Home Secretary would be entitled to consider the potential benefits of doing so at this juncture, against potential disadvantages in terms of influence and future relationships. A recent House of Lords Select Committee did not suggest that the Taleban should now be proscribed[98].

Other

3.20. The proscription list, which contains details of proscribed groups, is regularly updated. The last update was in November 2021[99]. It contains general information about proscription, including with the 5 "discretionary factors" to which the Home Secretary has regard in deciding whether to proscribe, assuming that the statutory test in section 3 Terrorism Act 2000 is met.

3.21. Updated guidance was also published during 2021 on appealing to the Proscribed Organisations Appeal Commission[100].

3.22. In November 2021, the Supreme Court heard an appeal on the flag-waving offence (section 13 Terrorism Act 2000)[101].

- The Supreme Court confirmed[102] that it was an offence of strict liability to display the flag of a proscribed organisation, and therefore it was not necessary that the defendant knew or intended that he was arousing any suspicion that he was a member of a proscribed organisation.

[95] Proscribe since 2015.
[96] Under the Afghanistan (Sanctions) (EU Exit) Regulations 2020.
[97] Section 3 Terrorism Act 2000.
[98] 2019-21 HL 218, supra.
[99] Home Office, 'Proscribed terrorist groups or organisations' (last updated 26.11.21).
[100] Home Office, 'Appeal against a ban on your organisation' (16.3.21).
[101] Pwr v Director of Public Prosecutions [2022] UKSC 2.
[102] Upholding the decision of the High Court in [2020] EWHC 798, Divisional Court, discussed in Terrorism Acts in 2019 at 3.3.

- This tough approach was justified by purpose of the prohibition: to deny proscribed organisations "the oxygen or publicity or a projected air of legitimacy", to stifle recruitment, and prevent disorder.
- The restriction on freedom of expression contained in the prohibition was justified as a "highly focused" provision to restrict or deter future violence.
- It was common ground that a defendant must know that he is wearing or carrying or displaying the relevant article, and to that extent a limited mental element was contained within the offence.
- It was relevant to whether a fair balance had been struck between the needs of society and the rights of individuals that the penalty was comparatively minor (no more than 6 months' imprisonment) [103].
- Quite how significant this final factor is may be context dependent. In April 2022 the European Court of Human Rights considered a conviction for displaying a photo of the PKK leader, Ocalan, and spreading PKK propaganda at a demonstration while marching on an unauthorised route. The Court held that there was insufficient link to terrorism or violence, and the sentence of 2 years 1 month was a disproportionate interference with the right of free association (Article 11)[104].

3.23. Following an adverse ruling by the Proscribed Organisations Appeal Commission in 2021[105], the Home Secretary was required to reconsider her decision not to de-proscribe the LTTE. In September 2021 the Home Secretary again refused to deproscribe, with the likelihood of further legal proceedings.

3.24. Illustrating the wider ramifications of UK proscription, in November 2021 the EU General Court upheld the European Union's listing of the LTTE, holding that the EU Council had been entitled to rely on the UK's proscription decision in 2001[106].

Terrorism without Groups

3.25. The internet, with its ready access to instructional manuals, and opportunities for like-minded socialisation with supporters across the world, reduces the budding

[103] At paras 26, 55, 68, 77.
[104] Silgir v Turkey, App.No. 60389\10 (29 April 2022)
[105] Arumugam v Secretary of State for the Home Department PC/04/2019, 18 February 2021.
[106] Judgement T-160/19.

terrorist's need to rely on terrorist groups, and so it is no surprise that the internet age demands new operational responses[107].

3.26. A succession of gun attacks in the United States shows that individuals do not depend on groups to execute their plans or propagate their legacy. Online fascination, meme culture, the existence of online repositories[108], and viral dissemination[109] allow isolated individuals to attain the identity of "saint" in the eyes of their chosen collective[110]. Through live-streaming of attacks such as Christchurch, violent acts can maintain their shocking freshness even after the perpetrator's death or incarceration.

3.27. The Chan sites have a history of attracting individuals drawn to violent imagery and words and are saturated by racism[111] and hostility towards women. These internet forums are not in themselves terrorist organisations: a Chan, for example, hosts a variety of 'imageboards' which may be dedicated to topics such as cooking, music and anime. The creation, moderation and content of imageboards are left to individual members.

3.28. '8chan' hosted the notorious imageboard '/pol/' (standing for politically incorrect), used by Brenton Tarrant to pre-announce his mosque attacks in Christchurch (New Zealand)[112], as well as the Poway Synagogue shooter[113]. Users may come and go, many of whom appear to be anonymous trolls and others looking for clicks[114].

3.29. When the Poway synagogue shooter made his announcement, he was told by another 8Chan user to 'get the high score'[115]. On these forums:

[107] Comerford, M., "Confronting the Challenge of 'Post-Organisational' Extremism", Observer Research Foundation, August 19, 2020, Observer Research Foundation (19.8.20). Hoffman, B., and Clarke, C., "The Next American Terrorist", The Cipher Brief, July 2, 2020.
[108] Such as archive.org.
[109] New Zealand Government, '2021 Digital Violent Extremism Transparency Report'.
[110] Ben Am, A., Weimann, G., 'Fabricated Martyrs: The Warrior-Saint Icons of Far-Right Terrorism', Perspectives on Terrorism vol.15 issue 5 (2020).
[111] Just one illustration: on 9.3.22 users on the site were offering free copies of 'Angry Goy: The Ethnic Cleansing Video Game'.
[112] Crawford, B., Keen, F., Suarez de-Tangil, G., 'Mimetic Irony and the Promotion of Violence within Chan Cultures' (Crest, December 2020).
[113] Evans, R., 'Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board' (Bellingcat, 28.4.19).
[114] Louis Theroux 's Forbidden America, BBC, 13.2.22.
[115] Evans, R., supra.

- Violence is both trivialised and glorified.
- Pop-cultural aesthetics, humour and irony are used to lower the barrier for participation.
- 'Gamification' of violence takes place[116].

3.30. The importance of these forums to US mass killers is undeniable. The Buffalo shooter, Payton Gendron, expressly stated in his 'diary' that he was radicalised by 4chan where he came across Tarrant's manifesto and found that he agreed with the contents[117].

3.31. Patrick Crusius, who carried out what appears to have been an anti-immigrant mass-shooting in El Paso, Texas, posted his manifesto on 8Chan[118].

3.32. Similar forums were used by Philip Manhaus who plotted to attack an Islamic Centre in Norway in August 2019 ('Endchan') and Stephan Balliet who attacked a synagogue in Halle, Germany in October 2019 ('Meguca')[119].

3.33. These forums engender a sense of belonging and community, where anonymous (and possibly sad and lonely) individuals can hang out enjoying transgressive entertainment with other users[120].

3.34. Part of this transgressive element is the idolisation of killers, such as Saint Tarrant[121] or, in the incel world, Saint Elliot Rodger[122]. This idolisation may involve copying apparently trivial details in previous attacks: the Poway shooter was so desperate to be identified with the Christchurch massacre that he claimed his own attack was funded by a YouTuber who had been namechecked by Tarrant[123].

---

[116] Crawford et al, supra.
[117] Sardarizadeh, S., 'Buffalo shooting: How far-right killers are radicalised online' (BBC, 17.5.22). I was able to access the 'diary' on 23.6.22.
[118] Stewart, E., '8chan, a Nexus of Radicalisation Explained' (*Vox*, 4.8.19)
[119] Crawford et al, supra.
[120] Thorleifsson, C., 'From cyberfascism to terrorism: On 4chan/pol/ culture and the transnational production of memetic violence', Nations and Nationalism Vol28 Issue 1 (2022).
[121] Ben Am, A., Weimann, G., 'Fabricated Martyrs: The Warrior-Saint Icons of Far-Right Terrorism', Perspectives on Terrorism, Vol 14, Issue 5 (2020).
[122] Hoffman, B., Ware, J., Shapiro, E., 'Assessing the Threat of Incel Violence', Studies in Conflict & Terrorism, 43:7, 565-587.
[123] Evans, R., supra.

3.35. In 2021 the government referred to individuals acting "out of a sense of duty, or a desire for belonging and those obsessed with massacre or extreme/mass violence without targeting a particular group"[124].

3.36. Being anonymous, users can establish an identity that may bear no relationship to their offline selves. The internet has allowed females to participate in online jihadi spaces; children to pretend to be adults; and users to play multiple roles (for example, Joshua Goldberg whose online identities included Nazi and jihadi)[125].

Limits to Proscription

Online Activity and Content

3.37. For online counter-terrorism, proscription unlocks action from the tech sector. The democratic standing of the UK, and the robustness of the proscription process (order made on the basis of careful internal analysis, followed by Parliamentary debate, subject to review by the Proscribed Organisations Appeal Commission, together with oversight by the Independent Reviewer of Terrorism Legislation), mean that proscription decisions are trusted and actionable conclusions about the nature of an organisation[126]. This means that content produced by these organisations should be removed from the internet.

3.38. However, the proscription power only applies to organisations[127].

3.39. It is correct that 'organisation' is widely defined to include any association or combination of persons[128], and this loose definition reflects the fact that terrorist groups are unlikely to have formal lists and standing orders. However,

- the organisation must have enough of a separate personality so that it, as opposed to any one or more of its members, can be said to be 'concerned in terrorism'.

[124] Home Office, 'Individuals referred to and supported through the Prevent Programme, England and Wales, April 2020 to March 2021' (November 2021).
[125] Conway, M., 'Understanding Online Radicalisation', Tech Against Terrorism, podcast (S2E4, 3.9.22).
[126] See further, Chapter 12.
[127] Section 3 Terrorism Act 2000.
[128] Section 121. R v Z, supra, at para 6, sets out the history of section 3 and the insertion of this statutory definition.

- On the assumption that it must be possible to be a 'member' of such an organisation[129], then this is likely to involve a degree of reciprocity with other members and a desire to further its aims[130].
- It does not apply to organisations who were once, but are no longer, concerned in terrorism. It cannot be used to address the enduring online legacy of a terrorist group that has ceased to exist.

3.40. It follows – to take the hypothetical example of a website that routinely encourages terrorism – that the Home Secretary would face formidable difficulties in using proscription because (a) he would have to be satisfied that an organisation, and not just an individual, was responsible for the website; and (b) assuming he could be satisfied that more than one individual was involved, he would have to be satisfied that an 'organisation', having some reciprocity between members and coherency of aims, was responsible.

3.41. It would be no solution for the Secretary of State to conceptualise 'the administrators of Website X' or 'those who post Y terrorist manifestos' as an organisation, unless it could be fairly said that the characteristics of reciprocity and coherent aims were present, and that it was understood to exist by those who involved in it. Otherwise, it would be unclear whether, by pursuing a particular course of conduct, an individual was or was not participating in the activities of a proscribed organisation.

3.42. It may be for this reason that, even for groups which operate predominantly online, proscription has only occurred after arrests of identifiable members for terrorism: the question of whether the group is responsible for a particular website, or for particular content, does not need to be answered in order to meet the statutory threshold.

3.43. The net effect is that the proscription tool is of limited assistance in countering online activity. Although UK proscription will continue provide a basis for tech company membership organisations (such as GIFCT or Tech Against Terrorism) to advocate content removal in relation to proscribed organisations, it is not a solution to:

[129] Section 11 criminalises membership of a proscribed organisation.
[130] R v Ahmed [2011] EWCA Crim 184, at paras 86-9.

- Websites or forums which encourage terrorism.
- The online activities of lone individuals or diffuse arrangements of individuals lacking the characteristics of an organisation.
- Content such as manifestos or live-streamed video made by dead or captured individuals who have committed notorious acts of violence.

3.44. It is a difficult question whether, assuming it is available on the facts, proscription is the right category of response where the predominant purpose is to encourage tech companies to remove associated content.

3.45. On the one hand, proscription under the Terrorism Act 2000 comes at a heavy cost to individual freedoms, putting association with and support for the proscribed organisation within scope of the criminal law. Using proscription for the predominant purpose of facilitating content removal risks trivialising a legislative tool which was originally enacted in response to the activities of armed groups in Northern Ireland.

3.46. If proscription started to be used against groups where there was never any intention for executive action in the form of arrests or other disruptive measures against real life individuals then (a) the deterrent and condemnatory force of proscription[131] might be weakened and (b) the police might face a difficult dilemma, as Northern Ireland has shown[132], if group insignia were displayed publicly and no action was taken.

3.47. On the other hand, proscription is routinely used against overseas groups where the prospect of criminal liability under UK law is remote. In accordance with the government's published list of discretionary factors [133], proscription may be appropriate considering "…the need to support other members of the international community in the global fight against terrorism." Part of this fight is addressing the risk of harm caused by the presence of certain content online.

Terrorism financing and web-hosting companies

[131] Walker, C., 'The Anti-Terrorism Legislation' (Blackstones, 3rd Ed) at 2.43.
[132] Terrorism Acts in 2019 at 9.35.
[133] Home Office, 'Policy paper: Proscribed terrorist groups or organisations' (updated 26.11.21).

3.48. Terrorist-operated websites rely on web-hosting companies, the domain-name providers and those forming part of the internet architecture.

3.49. If CT Police wanted to prosecute an internet company[134] for providing services to Islamic State or National Action, however small the payment[135], the options are limited. Unlike the United States[136], the UK has no offence of providing material support to a terrorist organisation[137].

3.50. Assuming that it was possible to show that a tech company provided services to an individual who they knew or reasonably suspected were acting on behalf of a proscribed organisation[138]:

- The Terrorism Act 2000 terrorist-financing offences are directed at the raising, use, and arrangements for use of monies for the purposes of terrorism[139], or at money-laundering[140].
- It is something of a stretch to argue that an individual or company which is paid to provide a service is engaged in one of these offences.
- Moreover, it is doubtful that paying for web services to propagate terrorist propaganda will in most cases amount to services "for the purposes of terrorism", since much propaganda will not amount to a threat of action within the meaning of "terrorism"[141].

[134] Based anywhere in the world. The terrorist financing offences have extraterritorial reach: section 63 Terrorism Act 2000.
[135] The sums payable for hosting or DDOS protection services are likely to be minimal – although there is no minimum amount for criminal liability under the Terrorism Act 2000.
[136] In United States v. Alhaggagi, 372 F. Supp.3d 1005, 1009 (N.D. Cal. 2019) it was common ground that creating social media and email accounts for Islamic State supporters constituted a provision of services to a foreign terrorist organisation. In US v Osadzinski USDC (Chicago) (18.10.21) the defendant was convicted on the basis that he designed computer script that allowed Islamic State propaganda to be more easily distributed.
[137] It is an offence to solicit non-monetary support under section 12 Terrorism Act 2000, but not to provide it.
[138] And assuming it was possible to find out which companies provided the services –websites may use 'masking' services that conceal this information.
[139] Sections 15-17. In O'Driscoll v SSHD, MPC [2002] EWHC 2477 (Admin), the High Court observed at para 26 that the section 16 offence "is about knowingly providing money or other property to support a proscribed organisation…".
[140] Section 18. Money-laundering depends on the money already being tainted by the time an arrangement comes into force: R v Montila and others [2004] UKHL 50.
[141] As defined by section 1 Terrorism Act 2000. The alternative would be to argue that promoting a terrorist publication was done for the benefit of a proscribed organisation and therefore for the purposes of terrorism within section 1(5) Terrorism Act 2000.

It is therefore difficult to see how a web-hosting company could be successfully prosecuted in the UK for providing services to an individual who it knew or suspected was acting on behalf of a proscribed organisation. The only possibilities appear to be (a) if the web-hosting company is based in the UK and knows or suspects that its customer is engaged in terrorist financing, but fails to make the requisite disclosure to a constable[142]; or (b) if the customer is designated under one of the UK's counter-terrorism financial sanctions regimes[143].

Aid Agencies

3.51. There is less to write about the impact of terrorism legislation on humanitarian and peace-building agencies from an online perspective.

3.52. Offline, the impact of counter-terrorism legislation and sanctions on aid work remains a constant feature in the landscape[144]. Recent UN Security Council Resolutions have been increasingly explicit about the need to safeguard humanitarian action[145], and UNSCR 2615 (2021) stated that activities which would otherwise engage the UN asset freeze are not prohibited where these are necessary to ensure the timely delivery of humanitarian assistance or to carry out other activities that support basic human needs in Afghanistan. I will consider UNSCR 2664 (2022), which went even further and established a general humanitarian 'carve-out', in next year's report.

3.53. Transparency and guidance about how terrorism legislation is intended to operate remains important for engendering confidence amongst the aid sector and the banks on whom they depend. The government has updated its 'For Information Note'[146].

[142] Section 19 Terrorism Act 2000.
[143] Such as the Counter Terrorism (Sanctions) (EU Exit) Regulations 2019. My review of these regulations was published by HM Treasury 15.12.22.
[144] See recently: European Commission, 'Commission guidance note on the provision of humanitarian aid in compliance with EU restrictive measures (sanctions)' (C(2022) 4486 final); UN Special Rapporteur on unilateral coercive measures, 'Guidance Note on Overcompliance with Unilateral Sanctions and its Harmful Effects on Human Rights' (2022); Eckert, E., 'Counterterrorism, sanctions and financial access challenges: Course corrections to safeguard humanitarian action' (2021) 103 International Review of the Red Cross 415
[145] Weizmann, N., 'Respecting international humanitarian law and safeguarding humanitarian action in counterterrorism measures: United Nations Security Council resolutions 2462 and 2482 point the way' (2021) International Review of the Red Cross.
[146] Home Office, OFSI/ HMT 'For information note: operating within counter-terrorism legislation, counter-terrorism sanctions and export control' (updated 11.10.21).

3.54. The Crown Prosecution Service has now published bespoke prosecutorial guidance on 'Humanitarian, Development and Peacebuilding Work Overseas'[147]. This recognises the operational challenges faced by relevant agencies, for example the fact that a proscribed organisation may form part of the actual or de facto government of a country or region where aid work is necessary. This fully responds to my recommendation for guidance in my first annual report[148].

3.55. Work is going slowly on improving the use of section 21ZA and 21ZB Terrorism Act 2000, provisions which are capable of authorising transactions which would otherwise give rise to a possible terrorist financing offence[149].

- Leaving aside the interests of humanitarian, development and peacebuilding agencies, and the interests of the Foreign and Commonwealth and Development Office which funds a great deal of their activity, effective use of these provisions is in the interests of counter-terrorism. The absence of a mechanism for exempting humanitarian activity could tip the balance against proscription in cases where a proscribed organisation was in control of a region, but no aid could otherwise be delivered without breaking the law.

3.56. I attended the annual meeting of the Tri-Sector Group in 2022. The TSG is now well-established and producing positive outcomes. I look forward to reporting more on the TSG in next year's annual report.

[147] Available on the CPS website.
[148] Terrorism Acts in 2018 at 3.66.
[149] See Terrorism Acts in 2019 at 3.34.

4. INVESTIGATING TERRORISM

Introduction

4.1. Counter-Terrorism Police often use general investigative powers that apply to all criminal offences[150]. An extra tier of powers exists under the Terrorism Act 2000 which do not turn on securing evidence for use in criminal proceedings. The very existence of a "terrorist investigation"[151] opens the door to the use of cordons[152], terrorist search warrants and production orders[153], customer information orders[154], and account monitoring orders[155].

4.2. These reflect the fact that counter-terrorism policing is particularly concerned with prevention of future harm. Powers to obtain information to check on and monitor terrorist risk are similarly available to the police in connection with TPIM subjects[156] and released offenders[157].

4.3. Not all investigations into terrorist offending are "terrorist investigations". Those who are only suspected of encouraging terrorism or disseminating terrorist publications – frequent instances of online terrorism – cannot be subject to a "terrorist investigation" [158], and in these cases police powers are more limited[159]. In practice, however, CT Police are unlikely to know the full extent of a person's activities – and suspected involvement in encouragement or dissemination may give rise to suspicions of involvement in other dangerous activity.

---

[150] For example, under the Police and Criminal Evidence Act 1984 or the Proceeds of Crime Act 2002.
[151] Section 32.
[152] Section 33
[153] Schedule 5.
[154] Schedule 6.
[155] Schedule 6A
[156] Para 8 Sched 5 TPIM Act 2011 enables police to apply for 'compliance' search warrants.
[157] Section 56A Counter-Terrorism Act 2008 provides for search warrants for checking the risk of offenders subject to the notification requirements of Part 4. Section 43A Terrorism Act 2000, recently inserted by the Police, Crime, Sentencing and Courts Act 2022, enables search warrants to be granted to check on the terrorist risk of any other offender on licence.
[158] Section 32(e) Terrorism Act 2000 expressly excludes an investigation of the commission, preparation or instigation of offences under sections 1 and 2 Terrorism Act 2006.
[159] Nor is the section 41 arrest power available: see Chapter 5.

4.4. Unless they act covertly[160], CT Police do not need special powers to access publicly available information on the internet (Open Source Intelligence, OSINT).

Electronic Data

4.5. A highly digitised society like the UK offers golden opportunities to private companies and public authorities alike to snoop on the population. Some digital information will be highly relevant to terrorist intention or capability. It has been said that the rapier of intelligence is preferable to the bludgeon of emergency powers such as house to house searches[161] – and it is correct that the impact of digital intrusion is gentler than a smashed doorframe and seized property.

4.6. Vast amounts of digital data, much of it personal, are obtainable by the intelligence agencies[162] in transit (for example through interception) or at rest (for example through the acquisition of bulk datasets[163]), or by the police from seized devices of ever-increasing capacity[164]. Most of the data any of us acquire is internet-related in some way: either downloaded or shared online. So great are the quantities that general police capacity is stretched. In February 2022 it was reported that over 20,000 devices await examination[165].

4.7. 'Discovery'[166] of online expressions about violence and ideological attachment may lead to operational dilemmas. A group of individuals could be discussing potential targets in an online group: this could represent a genuine threat to life, or objectionable and racist fantasy that will lead nowhere. The risks of over-reaction and resource

[160] And require authorisation for directed surveillance or the use of covert human intelligence sources under the Regulation of Investigatory Powers Act 2000.
[161] Omand, D., Phythian, M., Principled Spying: the Ethics of Secret Intelligence (Oxford, 2018).
[162] In April 2020 MI5 assumed full primacy for Extreme Right Wing Terrorism (ERWT) alongside its existing Islamist terrorist work: ISC, 'Extreme Right-Wing Terrorism', HC459 (2022), para 201.
[163] The agencies' use of Bulk Personal Datasets was first avowed in 2015: The Queen (on the application of Privacy International) v Investigatory Powers Tribunal [2022] EWHC 770 (QB), at para 9.
[164] Renwick, J. (Aus INSLM), 'Trust but Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters' (2020), at para 5.12 et seq ('What do our mobile phones say about us?').
[165] Channel 4 News, 'Police backlog of over 20,000 digital devices awaiting examination' (22.2.22).
[166] The word 'discovery' is a term of art. It describes the intelligence agencies' tools and methods used to identify individuals who may pose a risk, including online: ISC, supra, fn.281. Discovery has been deployed against suspected ERWT individuals by GCHQ (ibid, paras 238) and MI5 (Anderson, D., '2017 Terrorist Attacks – MI5 and CTP Reviews – Implementation Stocktake, Unclassified summary of conclusions' (11.6.19), para 8.21).

diversion are high: and the more stones are turned over online, the more potential terrorism is found.

4.8. The great majority of digital information that may be processed is, however, useless to counter-terrorism investigators. This is exacerbated the ease of data acquisition. The government has expressed its faith in developments in artificial intelligence to sort the wheat from the chaff[167].

4.9. That is not to say that all data is straightforward:

- Legitimate tools like encryption can be deployed by terrorists to frustrate investigations and avoid content removal[168].
- The international dimensions of cloud storage pose questions about the reach of terrorism and general policing legislation.
- Online anonymity poses major problems for countering terrorism online. Police refer to “attribution” – a process of matching user to account or content which may require detailed investigation. The result is that material giving a clue about a person’s intention may be discoverable on the internet, but the person behind the threat may remain invisible.
- The use of blockchain technology and cryptocurrency may complicate terrorist-financing investigations.

Impact and Legality

4.10. Where a person’s device is seized for examination, the most immediate consequence for them is the inconvenience of loss of access to emails, texts, frequently used apps, passwords and so on. Terrorism searches often result in the uplifting of every electronic device found on the person or in the premises, including devices which belong, or appear to belong, to children. Drawing a line between devices that should be seized, and those that can safely be ignored, is difficult.

4.11. The next consequence concerns privacy.

[167] Contest 3.0 (2018), para 190.
[168] Malik, N., 'Terror in the Dark: How Terrorists use Encryption, the Darknet, and Cryptocurrencies', Henry Jackson Society (2018).

4.12. Despite the volume of personal data rapaciously acquired by private companies, there is only a false equivalence to be made between the impact of surveillance capitalism[169], and the impact of data-gathering by police and intelligence bodies.

4.13. This is because, where personal data is gathered by the authorities, the stakes are higher. It is at least possible that the data gathered will be used against an individual, their family or friends in connection with watch-listing, travel-blacklisting, further surveillance, criminal investigation, examination under Schedule 7, or arrest. Privacy has been famously defined as a right to be let alone[170]. If so, then there is a particular right to be left alone by the authorities, unless the intrusion on privacy is justified.

4.14. These potential consequences explain why merely gathering personal data is considered, in law, to amount to an interference with privacy rights. Examination and use of that data will increase the level of that interference[171].

4.15. It is true that, for obvious historical reasons, the systematic recording of personal data by authorities concerned with state security has evoked different responses in the UK compared to continental Europe[172].

4.16. But in the United Kingdom, as in the rest of the Council of Europe Member States, the law recognises that the state's systematic collection and storage in retrievable form, even of public information about an individual, is an interference with private life[173], including in the case of data that is only readable by machines[174].

[169] Zuboff, S., 'The Age of Surveillance Capitalism' (Profile, 2019).
[170] Warren, S., Brandeis, L., 'The Right to Privacy', Harvard Law Review 4, no.5 (December 1890).
[171] At least for bulk data regimes. The European Court of Human Rights has understandably held that the level of interference increases as the process – from gathering, filtering, examination and dissemination of intelligence product – progresses: Big Brother Watch v United Kingdom, App.Nos. 58170/13, 62322/14 and 24960/15 (25.5.21), Grand Chamber, at paras 325, 331.
[172] R (T) v Chief Constable of Greater Manchester Police [2014] UKSC 35, per Lord Reed at para 88. Accepting that public attitudes may be ill-informed or hastily made, Lord Anderson QC's 'Question of Trust' (DATE) at 2.25 et seq has an interesting examination of public attitudes in this context.
[173] R (on the application of Catt) v Commissioner of Police of the Metropolis [2015] UKSC 9, per Lord Sumption at para 5.
[174] Big Brother Watch v United Kingdom, supra, at para 330.

Privacy rights are therefore invoked against state surveillance of personal communications, email[175] or bulk data[176].

4.17. These privacy consequences demand effective procedural safeguards which, in a case concerning police protest records, enable their deletion once their retention became disproportionate[177].

- Although systems holding data relating to CT investigations are designed with particular security, it is in principle possible that data gathered by authorities could be hacked. This would have significant practical and privacy consequences, and the risk of hacking is an additional reason for data deletion.

4.18. Given the privacy consequences of data gathering, the exercise of powers to gather and analyse data should be done so far as possible with the informed consent of the public. This may be termed the "social compact model"[178]. A run of cases before the Investigatory Powers Tribunal and the European Court of Human Rights[179] has given priority to the question of whether standards governing the use of powers are accessible and enforceable (referred to as legality).

4.19. Legality can be demonstrated in part by clear and detailed legislation about how and why data is gathered, backed by safeguards. Examples are the Investigatory Powers Act 2016 and its accompanying Codes of Practice and, during the year under review, the Covert Human Intelligence Sources (Criminal Conduct) Act 2021.

4.20. The benefit of legislation, unlike internal rules that are not visible to outsiders, is that it can be adjudicated upon by judges. In a fast-moving and uncertain environment, judges can "force debate" about the scope of powers and the adequacy of safeguards[180].

[175] Liberty and Others v The United Kingdom, App No 58243/00, Judgment, European Court of Human Rights (1 July 2008).
[176] Big Brother Watch v UK, App.Nos. 58170/13, 62322/14 and 24960/15 (25 May 2021, ECtHR, Grand Chamber).
[177] Catt v United Kingdom App.No. 43514/15 (24.1.19) at para 119.
[178]Omand, D., Phythian, M., supra.
[179] E.g., Big Brother Watch v UK, App.Nos. 58170/13, 62322/14 and 24960/15, Grand Chamber, 25 May 2021.
[180] Omand, D., Phythian, M., supra.

4.21. To a certain extent, compared to the Investigatory Powers Act 2016 the legality of less flashy modes of data acquisition and retention has fallen behind.

Remote Access

4.22. Remote access refers to police officers in one location (say, Liverpool) directly obtaining electronic data held in different location (for example, a server in Iceland).

4.23. The aspect of remote access considered here concerns the ability of CT Police, in possession of a seized device, to directly obtain data held in a different location *which is accessible from that seized device*. An example would be Dropbox files, accessible from a seized tablet device, but not previously downloaded. The need for this sort of access may increase:

- Some devices such as netbooks or Chromebooks operate principally as an interface with cloud-stored data, with limited data stored locally.
- Cloud-based smartphones - essentially a sheet of interactive glass with all data held remotely – are not out of the question[181].

4.24. Legislation governing investigative powers, including terrorism legislation[182], does not address remote access and in the case of searches of mobile phones under Schedule 7 is incompatible with it[183].

4.25. The principal exception is the Police and Criminal Evidence Act 1984 which enables police officers who are lawfully on premises (for example, under a Terrorism Act search warrant) to require information stored in electronic form which is "accessible from the premises" to be produced in a form which can be taken away [184]. This suggests (although views differ) that a police officer may access remote data whilst on searched premises.

[181] Menear, H., 'Could 5G give us a truly cloud-based smartphone' (Mobile, 10.11.20); Canonical blog, 'Vodafone Cloud Smartphone based on Anbox Cloud' (28.2.22).
[182] Section 43 Terrorism Act 2000 (search of person or vehicle), 43E (search of released terrorist offender), 47A (search of person or vehicle), Schedule 5 (search warrants), section 56A Counter-Terrorism Act 2008 (search of premises belonging to released terrorist offender), Schedule 5 TPIM Act 2011 (searches for TPIM compliance purposes).
[183] See Terrorism Acts in 2020 at para 6.48.
[184] Sections 19(4), 20(1).

4.26. Various workarounds are inconsistently used by different police forces, including intrusive powers under the Investigatory Powers Act 2016. The Law Commission found that some police forces sought cloud data under general search warrant powers[185] but noted that the more intrusive investigatory powers and their accompanying safeguards were not designed with routine police demand for remote access in mind[186].

4.27. It is true that some of the difficulties may be mitigated by treaty-based mutual assistance between countries. The state where the data is located or from where it is controlled may be requested to exercise its powers in support of a UK terrorism investigation[187]. But such assistance is time-consuming and depends on the existence of cooperative relationships.

- For US-held or controlled data, assistance is found in a recent agreement between the UK and the US, in force from October 2022[188]. This enables UK law enforcement authorities to obtain data directly from US service providers[189] underpinned in the UK by the Crime (Overseas Production Orders) Act 2019, and in the US by the CLOUD Act[190].

4.28. The question arises whether legislation is desirable, either for the purposes of terrorist investigations, or more generally, to enable police to access remote data. It is appealingly simple to provide that if an individual can access remote data from their device, the police should have a power to do so where that access can be justified.

4.29. In its report on Search Warrants, the Law Commission scoped out the issues but did not feel able to offer a solution to the remote access issue[191]. There are three facets of remote access which require particular attention if a legislative solution is to be found.

[185] Law Commission, 'Search Warrants', HC 852, Law Com No 396 (2020) at para 16.1.
[186] Ibid, at para 6.147.
[187] Under the Crime (International Co-operation) Act 2003.
[188] The Second Additional Protocol to the Budapest Cybercrime Convention, adopted by the Council of Europe on 17 November 2021, is intended to provide a similar platform for a wider range of countries.
[189] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington (3.10.19), CP 178.
[190] Clarifying Lawful Overseas Use of Data (CLOUD) Act.
[191] Ibid at chapter 16 (Search for and seizure of remotely stored electronic data).

4.30. Firstly, the question of whether remote access amount to an extra-territorial exercise of UK power needs to be considered.

- In answering this question, one can leave aside immediately the question of futility: it is ordinarily futile for one country to asserts its authority over subjects of another country[192] but that does not apply to remote access – it is to be assumed that access is technically possible from the seized device, and that any passwords will have been secured.
- However, under international law, backed up by more uncertain principles of international comity[193], states may not, absence the existence of a permissive rule to the contrary, exercise their power in any form in the territory of another state[194]. This includes the carrying out of official investigations in a foreign state[195], albeit identifying the limits of this 'enforcement' jurisdiction is difficult[196].
- It is in principle open to Parliament to legislate to authorise the exercise of law enforcement powers in an overseas jurisdiction[197] but (as shown by the Northern Ireland Protocol Bill) express authorisations of international law are rare and controversial.
- If remote access does amount to an exercise of enforcement jurisdiction whose exercise might run contrary to international law and/or comity, the UK would no doubt wish to consider the wider international implications of authorising unilateral remote access.
- In general states have dealt with access to overseas data through mutual assistance arrangements; attempts to create wider agreements on remote access, have not proven very successful[198].

[192] Al-Skeini and others v Secretary of State for Defence [2007] UKHL 26, per Lord Rodgers at para 45.
[193] Comity is something less than a rule of international law, based on neighbourliness, mutual respect, and the friendly waiver of technicalities; it is a species of accommodation between states: R (on the application of KBR Inc) v Director of Serious Fraud Office [2021] UKSC 2, at para 24.
[194] The Case of the S.S. "Lotus" (France v Turkey) (1927) PCIJ Series A- No 10.
[195] R (Smith) v Oxfordshire Assistant Deputy Coroner [2011] 1 AC 1 at paras 245 to 246.
[196] R (Jimenez) v First-tier Tribunal (Tax Chamber) [2019] EWCA Civ 51 at para 53 (Leggatt LJ).
[197] R (on the application of KBR Inc) v Director of Serious Fraud Office, supra, at para 21.
[198] The UN's Counter-Terrorism Committee Executive Directorate (CTED) has produced an excellent summary in 'The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives' (January 2022).

- The drafters of the Budapest Convention on Cybercrime (2001)[199] found it impossible to establish a comprehensive legally binding regime to regulate unilateral access to overseas data in the absence of mutual legal assistance.

4.31. Two recent domestic cases yielded different results on the extra-territorial question. In the first (*Jimenez*), the sending of an information notice to a UK taxpayer based in Dubai, reasonably required by HM Revenue and Customs to check his tax position, was held not to contravene any international obligation of the UK[200]. In the second case (*KRB Inc*), the imposition of an information requirement on an overseas company, backed by penal sanction, was found to have extra-territorial effect and the relevant statutory power did not extend that far[201].

4.32. Neither of those cases dealt with remote access. Remote access does not involve any requirement being placed on a person outside the jurisdiction. The transborder aspect in remote access cases arises where instructions sent from the UK (where the seized device is held) cause an overseas server to operate in pushing data held remotely onto the seized device[202]. Remote access involves direct law enforcement action to obtain the data rather than via a requirement placed on an individual or company.

4.33. There are good arguments that remote access is akin to the situation considered in connection with Article 32 of the Cybercrime Convention.

- Article 32 of the Convention sets out two situations in which all parties agreed that unilateral action was possible (in Article 32)[203]: firstly, where the information was publicly available; secondly, where the individual who is lawfully authorised to disclose data (for example, a person in the UK whose emails are stored in France) gives their voluntary consent.

[199] Which does not apply to terrorism offences: see the UK's Explanatory Memorandum on the Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CP 734.
[200] R (on the application of Jimenez) v First Tier Tax Tribunal and HMR, supra, at paras 49, 53
[201] R (on the application of KBR Inc) v Director of Serious Fraud Office, supra.
[202] No transborder aspect would arise if the data was held in the UK. Indeed, it may not be known in which part of the world the data is stored at any time (because data in the cloud may be moved between different locations), although the location of the controlling service provider is likely to be known.
[203] Council of Europe, Explanatory Report to the Convention on Cybercrime, ETS no.185 at paras 293-4, discussing Article 32.

- None of the drafters considered that remote access by law enforcement, at least with the consent of the person in control of the data, was a violation of international law. This suggests that some forms of cross-border access, even by law enforcement, does not offend against rules against extra-territorial enforcement.
- In *KBR Inc* it was common ground that the statutory information power under consideration[204] could have been used to compel a British registered company to produce documents held abroad by that company[205]. This can only have been because that type of requirement did not have an extra-territorial dimension within the curtilage of international law or comity.
- Widely drawn modern provisions in Australia's Crimes Act 1914 (Commonwealth) suggest that remote access is already accepted by some states[206].

4.34. Since remote access would only ever involve law enforcement activity from within the UK, acting in relation to a lawfully seized device within the jurisdiction, there is clearly a reasonable argument that remote access does not involve a breach of international law, and that new legislation should not be inhibited on that basis.

4.35. Secondly, any new power must cater for technical realities. When police secure remote access using a seized device they do not stand precisely in the shoes of the device's owner. Police need to guard against accidentally altering data held on a device, and also against interference or remote wiping – the demands of forensic integrity may require steps to be taken that would not occur to the owner of the device, for example by replicating the phone's access to the internet.

4.36. Thirdly, if remote access is generally permitted there is a danger of conferring an unbounded power on law enforcement.

- Where remote access from a seized device means access to literally anything that could be accessed from the seized device, the exercise becomes less a search of the device than a search of the cloud. The device itself becomes incidental. In *KBR Inc* the lack of "connection" between the UK and the overseas company was a

[204] Section 2(3) Criminal Justice Act 1987.
[205] Para 26.
[206] Sections 3F ('The things that are authorised by a search warrant'), 3CAA ('Account-based data') and 37QV ('Operating seized electronic equipment').

material factor in the Supreme Court's assessment that the power was being exercised extra-territorially[207].

- Some control on the nature of examination therefore seems necessary to keep a connection between the data sought and the device, and to minimise the risk of unjustified collateral conclusion[208]. Indeed, it is arguable that given the capacity of modern devices some controls should be imposed on examining locally held data[209].
- This argues in favour of establishing a further authorisation process that would delimit the nature of the remote search.

4.37. It is unlikely that any legislation could provide a statutory test for when data is "connected" to a seized device, but the sorts of factors in play might include: the nature of any apps downloaded on the seized device; whether the device owner had previously accessed the remote data in question, or class of remote data; whether access to remote data was part of the functionality of the device.

4.38. A power of remote access could then have the following characteristics.

i. The power would only be exercisable only if there was a connection or sufficient connection between the device in hand and the remote data being accessed. What this means in practice could be specified in a Remote Data Code.
ii. Subject to sufficient connection, the power would apply whether the data was held in the UK or not.
iii. Prior authorisation by senior officer or in judicial warrant would be required.
iv. Proof would be needed of safeguards against deliberate or inadvertent change of remotely held data.
v. The authorisation or warrant would need to specify so far as possible (a) the remote data to be looked for (b) the remote data's connection to the seized device
vi. The authorisation or warrant should be returned explaining whether obtained anything additional and (a) why that data was connected to the device and (b) why it was proportionate to do so.

[207] Para 59.
[208] The US Government's Note, 'Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act' (9.8.13), contains a fascinating description of how authorisations given to US authorities to examine bulk data limit the extent of analysis from an initial identifier or 'seed' (such as a phone number) to three steps or 'hops' within the data.
[209] Above and beyond the general controls within the Data Protection Act 2008.

4.39. In her response to last year's annual report, Terrorism Acts in 2020, the Home Secretary stated that she looked forward to seeing further analysis from me on remotely stored electronic data. The ball is now in the government's court.

Encryption

4.40. Access, whether local or remote, is a different matter where encryption is used. A description of encryption processes and the problems it poses to law enforcement is fully set out in the Australian Independent National Security Legislation Monitor's 9th Report[210]. As with remote access, the issues go far wider than terrorism – for example, encryption is relevant to the detection and investigation of Child Sexual Abuse Material (CSAM).

4.41. There are different types of encryption and it may be deployed in different context with different outcomes – for example, end-to-end encryption in the context of one-to-one messaging services is different from encryption in the context of social networks coupled to recommendation algorithms and promoted content.

4.42. Professor Sir David Omand, former director of GCHQ, and his co-author Professor Mark Phythian, identify encryption as a hard policy issue and note that:

> "…As with all hard public policy issues, there is no easy way of reconciling conflicting ethical concerns. Place the security of personal data and one's anonymity on the Internet above all else and law enforcement is shutout, the rule of law is undermined, and crime, terrorism, and cyber-attacks flourish. Insist on a right of access to all encrypted data to law enforcement and intelligence agencies - for example, through controlling or weakening encryption standards - and confidence in the Internet as a secure medium will be lost, and fragmentation of the Internet will spread." [211]

4.43. Another insider, the National Cyber Security Centre's former director, Professor Ciaran Martin, has set out the dilemma in similar, stark terms, concluding that if suitable technical compromise solution cannot be found between intelligence and online security, "…then security must win, and end-to-end encryption must continue

[210] Renwick, J., supra at para 5.38 et seq.
[211] 'Principled Spying: the Ethics of Secret Intelligence' (Oxford, 2018).

and expand, legally unfettered, for the betterment of our digital homeland" [212], ultimately at the expense of intelligence.

4.44. Those who take a sanguine view note that the golden age of electronic surveillance once existed but, thanks to encryption, is drawing to a close.

4.45. The difficulty, if it is a difficulty, is that privacy plays well in the market: consumers are naturally attracted to systems that guarantee that outsiders (whether public or private bodies) cannot access their data without their permission. It is unlikely that consumers fully contemplate the effects of exempting content from scrutiny, especially the impact on children exposed to CSAM and terrorism content.

4.46. This incentivises tech companies to design in processes which exclude anyone, even the platforms themselves, from accessing information and handing it over to law enforcement – incidentally removing the costs associated with law enforcement activity, and indeed reducing the burden of content removal[213]. Other technologies have similar effect: the platform Odysee claims that its blockchain technology prevents content from being removed[214].

4.47. CT Police and intelligence agencies will continue to try and find ways to compensate, and it will be suggested, accurately or not, that these other methods are sufficient[215] (for example, reliance on metadata, assuming it too is not encrypted[216]). It goes without saying that encrypted information can range from background intelligence to the targeting information for the next terrorist attack.

4.48. This is a complex field[217], and the purpose of this section of my report is to describe the issues rather than reach any recommendation. I note that my earlier

[212] 'End-to-End Encryption: the (Fruitless?) Search for a Compromise', Blavatnik School of Government, Oxford (November 2021).
[213] Unless the Online Safety Bill goes so far as to requiring the breaking of E2EE.
[214] Odysee, Terms of Service (updated: October 2021): https://odysee.com/$/tos (last accessed 15.9.22).
[215] Tech Against Terrorism, 'Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies' (2021); Herath, C., Dawda, S., 'Balancing End-to-End Encryption and Public Safety', RUSI (2022). Meta, the parent company of Facebook, has argued, in the context of its move to E2EE on its messaging services, that content moderation is not the be-all and end-all: 'Human Rights Impact Assessment on Meta's Expansion of End-to-End Encryption' (2022).
[216] So-called DNS over HTTPS.
[217] Muffett, A., 'A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022': https://alecmuffett.com/alecm/e2e-primer/e2e-primer-web.html#the-field-model-and-the-historical-mundanity-of-privacy (last accessed 15.9.22).

accepted recommendation[218] that consideration should be given whether new or adapted powers are required to compel suspects to hand over encryption keys[219] remains stuck at the consideration phase. This may because CT Police find existing powers workable despite their limitations; I look forward to seeing the outcome of the government's further consideration.

Retention

4.49. I have already explained how retention of data by CT Police has, and is considered by the law to have, an impact on individuals.

4.50. In last year's annual report, I made specific reference to the retention of phone data following a Schedule 7 examination, and called for greater clarity on the data journey. It ought to be possible for an individual whose phone or other device is downloaded to have some accurate understanding of how their data will be handled in general terms, including any safeguards.

4.51. The retention issue goes wider than the exercise of terrorism powers, but it does have a special relevance: terrorism investigations tend to be more exhaustive, sucking up more megabytes of data from more devices, than other types of investigation, and tend to happen on the basis of feared harm which may never take place. Suspicions, though worth investigating, may prove to be unfounded.

4.52. Relevance is problematic. A piece of data such as a phone number, and its connection to another phone number, may appear to have no relevance until it is attached to other information, perhaps many years later[220]. This could argue in favour of obtaining and retaining all data for ever, just in case, perhaps subject to safeguards controlling access (such as permission from authorising officers or a judicial officer). However:

- The social compact model demands that if that is the case, the privacy consequences of perpetual retention be debated and justified by the adoption of clear legislation.

[218] Terrorism Acts in 2019 at 4.30.
[219] Currently under section 49 Regulation of Investigatory Powers Act 2000.
[220] Cf. R (II) v MPC [2020] EWHC 2528, para 59, 74 in the context of Prevent data.

- The wider consequences for UK policing would have to be addressed: society has never conferred on law enforcement the power to do whatever it takes, to mitigate a risk, however small.

4.53. On the other hand, it must be acknowledged that an effective weeding and destruction process is difficult to construct. By way of hypothetical example:

- CT Police seize close to 200 devices from a home address connected to a terrorist suspect[221], including memory sticks and children's phones.
- Since there is no way of saying that a particular device cannot be relevant to the suspect's communications and contacts (for example, a children's phone could the source of key evidence) the contents of all the devices will be downloaded and analysed.
- After conviction, the data is likely to be retained for use in further terrorist investigations.
- In the medium term, assuming the contents are not being worked on, the data will be put into deep storage.
- Assuming that the data is not called for, some form of periodic review is then required.
- Since it is impossible to carry out a review whilst data is in deep storage, the data will need to be reloaded onto systems where it can be read.
- Given the quantities of data, some form of automation is likely to be required, but the boundaries for retention or deletion require some degree of human assessment: do CT Police retain *all* the contents of those devices that the terrorist can be shown to use (or where use cannot be ruled out)? Or do CT Police only retain the data on the devices that can be shown to be relevant, or the classes of data that have proven relevant in the past (for example, contact numbers but not photos)?

4.54. The government has accepted my recommendation last year to review the retention, review and disposal (RRD) timeframes for electronic data obtained from Schedule 7 examinations. I look forward to considering the outcome of that consideration in next year's report, noting that the need for clarity about RRD applies to all types of CT investigation.

[221] This number is based on a real operation.

Legal Professional Privilege (LPP)

4.55. The capaciousness of devices entails a risk of discovering the unexpected. It sometimes happens that investigators reviewing a device come across electronic data that appear to be privileged.

4.56. In such cases, CT investigators at NDES[222] have developed the following practice, based on the concept that a mobile phone or its forensic image is a 'single item'[223].

4.57. According to this practice, where LPP material is suspected to be present, the entire device is locked down, and no further examination takes place until measures can be taken to filter out both the suspected LPP material and any further potential LPP material. This may requirement the instruction of independent legal counsel.

4.58. Only once the process of isolation has taken place does examination then recommence. This delay can impede investigations with obvious implications for public safety; it could, in some circumstances, result in longer periods of pre-charge detention for individuals who have been arrested under section 41 Terrorism Act 2000 whilst remedial steps are taken.

4.59. CT Police raised the point with me, and I undertook to consider the matter further.

4.60. It is right that CT Police recognise the importance of excluding LPP material from their investigations. However, the practice that has developed appears to go further than is required.

4.61. Honouring the principle that LPP material is excluded from powers of search or seizure is not unique to CT Police.

[222] See Chapter 1.
[223] Law Commission, Search Warrants, supra at para 14.42 et seq. A device as a single item is analogous to a book; rather than a filing cabinet containing millions of separate items.

4.62. The general principle has been authoritatively explained by the High Court[224]: the seizing authority has a duty to devise and operate a system to isolate potential LPP material from the other material lawfully in its possession. This must reasonably be expected to ensure that such material will not be read by members of the investigative team before it has been reviewed by an independent lawyer to establish whether privilege exists.

- This principle is reflected in the Attorney General's Guidelines on Disclosure which require that where suspected LPP material is unexpectedly discovered when reviewing material, it must be isolated from the other material, and then reviewed by an independent lawyer[225].
- To discover if further LPP material exists, search terms may be applied by a member of the same law enforcement body, so long as they are independent of the investigation[226].
- If suspected LPP material is identified, it may only be examined by a lawyer who is independent of the police or any prosecuting authority[227].

4.63. There is therefore no requirement that, if suspected LPP material is discovered, the entire device is locked down. If for example a text message is found which, unexpectedly, appears to contain legal advice from a solicitor to his client, examination of the device may continue, as long as the suspect text message is excluded, and reasonable steps are taken to isolate any other potential LPP material.

4.64. This could, for example, involve investigators continuing to look at images and contacts, but ceasing to look at text messages or Word documents, until a police examiner who is independent of the investigation, has run reasonable search terms to identify whether other LPP material is present.

4.65. Assuming that the Attorney General's Office, as custodians of the Attorney General's Guidance, does not dissent from this analysis, I **recommend** that CT Police establish a new practice for dealing with unexpected LPP material that does not involve the locking down of the entire device.

[224] R (on the application of McKenzie) v Director of the Serious Fraud Office [2016] EWHC 102, at para 34.
[225] Updated May 2022, at para 28.
[226] McKenzie, supra, at paras 16-18.
[227] Para 29.

Post-charge questioning

4.66. Section 22 of the Counter-Terrorism Act 2008 contains an exceptional power to interview a person who has already been charged with a terrorism offence, or an offence that appears to be terrorism-connected. Questioning may be done under caution, with the risk of adverse inferences if the person fails to answer questions.

4.67. During 2021, this power was exercised on one occasion. Since criminal proceedings are still ongoing, I will report on the details of this case in next year's report.

Stop and Search

Section 43 Terrorism Act 2000

4.68. Section 43 Terrorism Act empowers a police officer to search a person on foot or in vehicles on reasonable suspicion that they are a terrorist.

4.69. The figures on the use of section 43 are only reported by the Metropolitan Police Service.

4.70. In 2021, 383 persons were stopped, of whom 27 were arrested. This is a fall from 2020 (524, and 57 respectively), and is the lowest number since 2011 when records began[228].

4.71. There has been a corresponding fall across all ethnicity categories of those stopped: 113 White people, 9 people of mixed ethnicity, 33 Black people, 72 Asian people, 23 'Chinese or other', and 133 whose ethnicity was not stated.

4.72. I am pleased that my recommendations on improved ethnicity data have been accepted by the government:

[228] Home Office, Statistics on the operation of police powers under the Terrorism Act 2000 and subsequent legislation, Year to December 2021: Annual Data Tables, Table A-S.01.

- The ethnicity categories for section 43 have in increased from six to seventeen. Particularly important is the disaggregating of the 'Chinese or other' category, so that there are no separate figures for Chinese people and Arab people.
- At the same time the Home Office is working with CT Police to see whether it is possible to collect data without relying on individual self-defining (which many people are, completely understandably, reluctant to do).

"Auditors"

4.73. This unusual and online-related topic was drawn to my attention whilst preparing for this year's report.

4.74. For some years, founding themselves on principles of transparency and accountability and imitating a practice developed in the United States, members of the public have acted as 'auditors' of police locations and sensitive locations such as the MI6 building. This involves filming locations or individuals on cameras or mobile phones and posting the footage online.

4.75. This practice has increasingly led to exchanges between auditors and the police. The culmination of some of these exchanges has been the use of section 43 Terrorism Act 2000. In October 2022 a police inspector was convicted of assaulting a 16-year old auditor outside Merthyr Tydfil police station in August 2021[229].

4.76. From the point of view of the auditor, the use of section 43 is disingenuous: there is no genuine police suspicion that the auditor is a terrorist, and the use of the terrorism power is nothing less than an attempt to deter lawful citizen activity. On occasion the police have made apologies or paid damages for the wrongful use of section 43 against auditors[230].

4.77. From the point of the police, the possibility that someone, whether the auditor, or a subsequent online viewer, will make sinister use of the information gleaned to carry out an act of violence or even a terrorist attack, cannot be ignored. From their perspective, questioning 'auditors' robustly and, on occasion making use of the section 43 power, is protective security at work. In Northern Ireland, it would be no

[229] 'Police inspector Dean Gittoes guilty of assault on teen' (BBC News, 5.10.22).
[230] E.g. 'Police make grovelling apology to Youtuber Auditing Britain over Kidderminster arrest video', Birmingham Live (14.1.22).

great step to conclude that filming the back of a police station was for targeting purposes, justifying the use of section 43.

4.78. Some protective concerns are likely to be dealt with by provisions in Part 1 of the National Security Bill. If passed by Parliament, these provisions will enable the police to require individuals to stop inspecting (directly or remotely) "prohibited places" [231] . There is already an arrestable offence of eliciting, publishing or communicating information about members of the armed forces, the intelligence services, or constables of a kind likely to be useful to a person committing or preparing an act of terrorism[232].

4.79. I have discussed this matter with CT Police.

4.80. Guidance currently issued to police officers in England and Wales is not in my view sufficiently clear that section 43 can only ever be used to search a person whom the officer "reasonably suspects to be a terrorist"[233]. It is not sufficient that footage, once posted, might be useful to another person – it is necessary to consider the suspected intention and state of mind of the individual[234].

4.81. On the other hand, Police Scotland have issued clear helpful and publicly accessible guidance[235].

4.82. In these circumstances I **recommend** that improved guidance is issued to police forces in England and Wales. It is up to police forces to decide on the form of that guidance, but I consider that the Police Scotland document is useful guide for police who encounter 'auditing' for the first time, and is clear about the limited circumstances in which section 43 powers are available.

4.83. I further **recommend** that consideration is given to whether individual forces should report on their use of section 43, for publication in official statistics. Whilst I

[231] Clause 6(1).
[232] Section 58A Terrorism Act 2000. It is a defence to prove that there was a "reasonable excuse" for the action concerned (58A(2)).
[233] Section 43(1). "Terrorist" is defined in section 40.
[234] In R (Miranda) v Secretary of State for the Home Department and another [2016] EWCA Civ 6, the Court of Appeal rejected the proposition that terrorism could be committed inadvertently (at paras 53 to 55).
[235] 'Auditors and Social Media Bloggers – Interim Guidance': https://www.scotland.police.uk/spa-media/ngulpset/22-0731-data.pdf (last accessed 20.9.22).

appreciate that most counter-terrorism powers that are reported on are exercised by CT Police, which facilitates the gathering of data, the purpose of statistics is to enable scrutiny of the power. It matters not to the public whether section 43 is deployed by a CT officer, or a neighbourhood officer. The fact that damages have been awarded for misuse suggests that scrutiny is warranted.

Section 47A

4.84. In my first report, I drew attention to uneven regional authorisation of no-suspicion stop and searches under s47A Terrorism Act 2000[236]. This exceptional power, rarely used in the UK, was exercised by 4 police forces in the aftermath of the Parson's Green attack in September 2017 when the national threat level was briefly raised to critical. For a short period of time it authorised police officers to exercise stop and search powers without suspicion within identified areas.

4.85. Authorisations were made by senior officers of British Transport Police; City of London Police; West Yorkshire Police; and North Yorkshire Police. The last two authorisations stood out because no other regional force (other than the City of London Police) considered them necessary.

4.86. My recommendation was that CT Policing should consider providing national advice to forces on the use of s47A[237] and this was accepted by the Home Secretary. She noted that the police would provide authorising offices with additional training and would work on a "central narrative" to ensure consistency, necessity, justification and proportionality in the use of the power[238].

4.87. I can report that CT Police have now developed a centralised advisory system, addressed to authorising officers[239], and their tactical advisers, on the circumstances in which a s47A authorisation should be considered.

- Advice is given by the Protect and Prepare wing of the CT Policing Network who are concerned with the protective security of people and places.

[236] Terrorism Acts in 2018 at 4.14 et seq.
[237] Ibid, at 4.18.
[238] Home Office, 'Response to Terrorism Acts in 2018' (22.10.20).
[239] Assistant Chief Constable or above.

- This is because s47A relates to locations which may be subject to attack, rather than to known or suspected individuals[240].

4.88. I can further report that, under local response plans, police forces are not to consider section 47A as a default option in response to the raising of the national threat level to critical[241].

4.89. I also recommended that the 2012 Code of Practice should be considered for updating. An amended Code of Practice has now been published which makes it clear that a general high threat from terrorism (including when the national threat level has been raised to critical) should not form the sole basis for authorising the use of section 47A[242].

4.90. The 47A power was not used in 2021.

Cordons

4.91. 7 cordons were erected under section 33 Terrorism Act 2000 in 2021 (up from 5 in 2020). The majority (7) were done by the Metropolitan Police Service[243].

4.92. Although the government accepted my recommendation that the power to search premises within a cordon without a search warrant should only be available in urgent cases[244], I am told that no suitable legislative vehicle has yet arrive to amend Schedule 5 of the Terrorism Act 2000. I hope to report next year that a suitable vehicle has been found.

Search warrants

[240] An authorisation is given "in relation to a specified area or place" and the specified area of place must be "no greater than is necessary to prevent" the suspected act of terrorism: s47A(1).
[241] By reference to local response plans that police forces are required to formulate.
[242] Revised Code of Practice (26.10.22).
[243] Home Office, Statistics on the operation of police powers under the Terrorism Act 2000 and subsequent legislation, Year to December 2021: Annual Data Tables, Table A-S.06.
[244] Terrorism Acts in 2018 at 4.27.

4.93. Work on the National Security Bill, which introduced a new power of search and seizure in urgent cases[245], and was modelled on Schedule 5 of the Terrorism Act 2000[246], identified the following point.

4.94. It is in theory possible, although never done in practice, for the police to obtain access to special procedure and excluded material in urgent cases without judicial – or other independent and impartial – scrutiny. This material includes confidential journalistic material and so raises the question of whether sufficient safeguards exist.

4.95. The equivalent power in the National Security Bill, if enacted by Parliament, will provide for ex post facto judicial authorisation (or not) for any confidential journalistic material seized in urgent cases[247]. This safeguard is modelled on provisions relating to border examinations in the Counter-Terrorism and Border Security Act 2019, which were enacted following the seizure of journalistic information from David Miranda at Heathrow Airport in 2013 under Schedule 7 Terrorism Act 2000 and ensuing judicial decisions[248].

4.96. I agree that nothing in Schedule 5 excludes the possibility of seizing journalistic material in cases of urgency and the point is not addressed in the relevant Code of Practice[249]. I am not surprised that this issue has not been identified before, but the new National Security Bill clauses beg the question whether a similar authorisation system ought to be created for journalistic material which is seized under the urgent search provisions of the Terrorism Act 2000.

4.97. This does raise the spectre that by formalising an authorisation process, journalistic material will start to be seized when it has never been seized (I am reliably informed) in the past.

4.98. The alternative is simply to provide, through amendment to the search Code of Practice, that officers may not seize and view journalistic material when acting under the urgent search power in Schedule 5. This was the approach taken after the Miranda case with respect to Schedule 7 Terrorism Act 2000[250]. It is interesting that the

[245] Para 10 of Schedule 2.
[246] Para 15 of Schedule 5 and, in Scotland, para 31.
[247] Para 11 of Schedule 2.
[248] Culminating in R (on application of Miranda) v Secretary of State for the Home Department [2016] EWCA Civ 16.
[249] Revised Code of Practice PACE Code A (December 2014).
[250] Schedule 7 revised Code of Practice, para 67.

government did not identify an operational need for police to have access to journalistic material when using the Schedule 7 power despite the facts of the Miranda case.

4.99. The case for creating a post-seizure authorisation process in Schedule 5 is really based on consistency with the National Security Bill. However:

- It is questionable to what extent consistency with the National Security Bill is desirable. The Bill has been drafted with considerable flexibility so as to deal with what is understood to be the amorphous and complicated threat arising from state threats.
- By contrast, terrorism is well understood and to date CT Police have not found themselves having to seize journalistic material in the course of urgent terrorism searches.
- This type of amendment to terrorism legislation is best approached incrementally, starting from the question of whether there is a genuine operational need.
- The principle that journalism should be protected in a democratic society is too important to allow developments by analogy.

4.100. I therefore **recommend** that the Code of Practice should be amended to specify that journalistic material should not be seized or viewed. It is the most effective protection for journalistic material since it exempts the material from the search power. It does not raise the spectre, hitherto never even considered, that the police are going to seize journalistic material. It provides parity with the search power under Schedule 7. There is no operational case for creating a novel judicial oversight mechanism, which is found nowhere elsewhere in terrorism legislation.

Biometrics

4.101. In his latest annual report[251], the Biometrics Commissioner has referred to the continuing difficulty with foreign holdings of biometric information extracted from the Interpol System. This aspect of police practice came to light because of Brexit, after which the UK's live access to the EU SIS II database lapsed.

[251] Commissioner for the Retention and Use of Biometric Material, Annual Report 2020 (2021).

4.102. A question arises as to whether the National Security Determination (NSD) process under Part 1 of the Counter-Terrorism Act 2008, which applies to biometrics obtained under Schedule 7, can be used to authorise the retention of biometrics from Interpol. Biometrics can play an important and sometimes central role in terrorist investigations.

4.103. At present, the 2008 Act makes no distinction between domestic and foreign holdings[252].

4.104. Having visited CT Police's biometrics unit where I was briefed on the number of red or blue Interpol notices containing biometrics data relevant to terrorist suspects, and inspected examples of these notices, and compared these with the material available in connection with domestic holdings, my view is that the National Security Determination (NSD) process is unsuited to these foreign holdings.

4.105. Firstly, the amount of relevant biometrics available through the Interpol system would overwhelm the NSD system.

4.106. Secondly, the detail provided in red or blue notices, and the use of foreign languages on many entries, means that making a rational NSD decision would require the UK to seek further information from the originating state. The Interpol database is not designed with these sorts of further inquiries in mind. Even assuming the originating state was willing to cooperate with an additional layer of process on top of Interpol's own rules and processes, to seek further information risks betraying sensitive UK investigations and could result in adverse inferences being drawn by that country about the person under consideration.

4.107. Thirdly, material drawn from Interpol is only held by UK authorities for as long as it is held on the Interpol system. In other words, the control over the retention of this set of biometric data is the Interpol system, governed by its procedures and agreements, not the UK.

4.108. This fact that data is entered onto the system in accordance with Interpol standards is, I believe, the answer to legitimate questions about the nature of the originating country which could in principle, applying corrupt or unfair standards, take

[252] Section 18(1).

biometrics material and seek to enter it on the Interpol database for illegitimate purposes. Creating a schedule of 'good' and 'bad' originating countries would be inconsistent with the Interpol system, and lead to invidious and probably arbitrary distinctions having to be made.

4.109. The European Court of Human Rights has recognised, in the context of bulk intelligence, that different considerations apply to intelligence gathered domestically, and intelligence shared by overseas partners[253].

4.110. There is some urgency in reforming the law in this area to make it clear that the NSD process does not apply to foreign Interpol holdings. CT Police are in possession of biometrics, held beyond 3 years but not subject to an NSD for its continuing retention. Although the pot is deliberately unsearchable, the data is still held. Pending any amendment to the law, it is incumbent on CT Police to identify a lawful basis for holding this material (and they may already have done so). It should never be said for data, or any other aspect of CT investigations, that following the law can be dispensed with in the greater public interest.

4.111. I therefore **recommend** that steps are urgently taken to exempt Interpol biometric holdings from the NSD regime under Part 1 of the Counter-Terrorism Act 2008.

Production Orders

4.112. CT Police Headquarters ('CTPHQ') have provided me with the following statistics. In 2021 CT Police applied for 81 production orders under the Proceeds of Crime Act 2002, and 37 production orders under Schedule 5 Terrorism Act 2000 all of which related to information already in existence[254].

4.113. In previous reports I have considered the use of production orders for journalistic material. I am not aware of any such cases in 2021. My recommendation that first instance judgments on these cases should be made available is still subject to consideration of whether and how it can be practically implemented.

[253] Big Brother Watch v United Kingdom, supra, at 473 et seq.
[254] Under para 7(1)(a) an order may be made with respect to material which is expected to come into existence within 28 days beginning with the date of the order.

Financial Investigations

Disclosure Orders

4.114. CT Police applied for 66 disclosure orders in terrorist financing investigations[255] during 2021.

4.115. Section 22B Terrorism Act 2000 provides a power to require further information about disclosures. The government proposes to amend section 22B to enable orders to be sought for information for strategic analysis of terrorist financing (following a recommendation by the Financial Action Task Force)[256]. The Bill is right to provide for a Code of Practice for the use of this power, to avoid fishing expeditions.

Customer Information Orders, Explanation Orders and Account Monitoring Orders

4.116. There were 88 Customer Information Orders, Explanation Orders or Account Monitoring Orders[257].

Suspicious Activity Reports (SARs)

4.117. In 2021[258]:

- 798 Terrorism Act 2000 SARS were disseminated.
- 271 Proceeds of Crime Act 2002 SARS disseminated that were identified as potentially relevant to terrorism.
- 269 SARS were disseminated that contained a request for a defence against terrorist financing[259].
- (as of July 2021) 48 of these were refused.

Cryptoassets

4.118. Crypto-assets are an online phenomenon.

[255] Under Schedule 5A. Source: CTPHQ.
[256] Through clause 146 Economic Crime and Corporate Transparency Bill.
[257] Under Schedules 6, 5 and 6A respectively. Source: CTPHQ.
[258] Source: CTPHQ.
[259] Under sections 21ZA or 21ZB Terrorism Act 2000.

4.119. In July 2021, Hisham Chaudhary was convicted of using Bitcoin to support Islamic State[260]. In December 2021, a released terrorist offender was sentenced to 16 months' imprisonment for failing to disclose his use of internet accounts to trade cryptocurrency[261].

4.120. Given that terrorists continue to adapt to new technologies[262], finding ways to track crypto transactions could be a rich source of information on terrorist groups (such as Hamas, who have previously posted an online call for Bitcoin[263]) and, potentially, on self-activating terrorists[264].

[260] 'Sales consultant guilty of Bitcoin Islamic State terrorism funding' (BBC News, 6.7.21).
[261] Contrary to Part 4 Counter-Terrorism Act 2008, R v Iqbal, 21 December 2021, Central Criminal Court.
[262] Malik, N., 'Terror in the Dark: How Terrorists use Encryption, the Darknet, and Cryptocurrencies', Henry Jackson Society (2018); Keatinge, T., & Danner, K., 'Assessing Innovation in Terrorist Financing', Studies in Conflict & Terrorism, 44:6 (2021).
[263] Bauer, K., Levitt, M, 'Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat', The International Centre for Counter-Terrorism – The Hague (ICCT) Evolutions in Counter-Terrorism, Vol. 2 (November 2020); Wilder, H., 'An overview of the use of crypto currencies in terrorist financing' (Coinbase, 2021).
[264] Reimer, S., Redhead, M., 'A New Normal: Countering the Financing of Self-Activating Terrorism in Europe', RUSI (May 2021). However, the authors have suggested that there remains overall uncertainty about the role played by crypto in terrorist financing: Reimer, S., Redhead, M., 'Bit by Bit: Impacts of New Technologies on Terrorism: Financing Risks' (RUSI, 2022).

5. ARRESTING AND DETAINING

Arrests in 2021

5.1. There were 186 terrorism-related arrests in 2021 (down from 188 in 2020), the lowest figure since 2011[265].

5.2. Section 41 Terrorism Act 2000 is a special arrest power that can be used to detain a person who is reasonably suspected to be a terrorist for as long as 14 days, pre-charge[266].

- A "terrorist" is a person who has either committed a specified terrorism offence, or who is or has been concerned at any time in the commission, preparation, or instigation of acts of terrorism[267].
- Of note, the list of specified terrorism offences does not include two of the terrorism offences most often committed online: encouragement, and dissemination of terrorist publications[268].
- If an individual is only suspected of committing these offences, the section 41 arrest power is therefore not available, although in practice CT Police may have wider suspicions about what the individual is up to.

5.3. The other arrest power is the general power to arrest on suspicion of an offence under the Police and Criminal Evidence Act 1984 ('PACE'), the Criminal Justice (Scotland) Act 2016 and the Police and Criminal (Northern Ireland) Order 1989.

5.4. In practice, CT Police in Great Britain use PACE powers of arrest far more frequently than section 41.

- In 2021, out of 186 terrorism-related arrests in Great Britain, only 32 (17%) were under section 41. This is the second lowest ever (the lowest was 26 in 2020)[269].

[265] Home Office, Operation of police powers under the Terrorism Act 2000, Year to December 2021: Annual Data Tables, Table A-A.01.
[266] Code H is the Code of Practice dealing with arrests and detention under section 41.
[267] Section 40.
[268] Sections 1 and 2 Terrorism Act 2006.
[269] Table A-A.01.

5.5. One of the advantages of a PACE arrest is that, unlike section 41 Terrorism Act 2000, a person can be released on bail. This has obvious advantages for the younger potentially less risky cohort of individuals who now form a significant part of CT Police's caseload. Conversely, CT Police typically use section 41 where they assess there may be a need to detain an individual pre-charge until sufficient evidence to charge is obtained.

5.6. The outlier is Northern Ireland (see further Chapter 9) where section 41 is always used for terrorist-related arrests.

5.7. In 2021, the characteristics of the individuals subject to terrorism-related arrest were as follows (figures for 2020 are in brackets)[270]:

- 178 (167) men and 8 (19) women.
- 20 (19) children.
- For adults, 18 (20) aged 18-20, 18 (22) aged 21-24, 33 (34) aged 25-29, and 97 (92) over 30.
- 95 (90) White people, 10 (16) Black people, 40 (64) Asian people, 41 (18) other people[271]. Although 2020 was close, this is the first time that there have been more terrorism-related arrests of White people than of all the other categories put together.
- 146 (143) British.

Children in 2021

5.8. The number of children arrested in 2021 (20) is the largest ever, apart from the multiple-attack year of 2017.

5.9. All but one were suspected Extreme Right Wing Terrorists[272].

[270] Tables A-A.09, A-A.10 and A-A.11.
[271] The government has accepted my recommendations to improve the ethnicity categories and, from December 2022, proposes to increase the categories for the arrest figures.
[272] Assistant Commissioner Matt Jukes, quoted in 'Far right "mimicking video games to lure middle class children to terrorism"' (Guardian, 17.3.22).

- During 2021 only 5 children were eventually charged with terrorism-related activity[273]. For those who were not charged, either there was insufficient evidence of a terrorist offence, or the public interest did not warrant prosecution.
- At least one of the children arrested was very young. In July a 14-year-old boy from Darlington with "complex vulnerabilities" was arrested after becoming obsessed with school shootings online[274].

5.10. During 2021 Counter Terrorism Policing released 54 news items on their website[275]. In 10 of these, the police drew attention to the risk posed to children by online terrorism content and asked for vigilance.

5.11. In his 2021 threat assessment, the Director-General of MI5 referred to a "high prevalence of teenagers including young teenagers"[276].

5.12. Overstating the coherency or 'blockiness' of Extreme Right Wing Terrorism as manifested by children is to be avoided.

- There are rather certain dominant themes (attitudes towards government, Jews, immigrants, women, and the importance of James Mason's neo-Nazi text 'Seige').
- Children's terrorist ideologies have been classified more frequently by Prevent (outside the context of arrest) as Mixed, Unclear and Uncertain[277]
- In the case of children, it is legitimate to question to what extent, if any, their views (however aggressively held) are to be equated with programmatic views for the transformation of society, as opposed, for example, to hate crimes[278].

5.13. Nonetheless, the fact that so many children are being arrested is important.

[273] Table A-A.10. It is possible that some of the 5 had been arrested in 2020, so it does not necessarily follow that 5 of the 20 children arrested were charged.
[274] 'Darlington teenager avoids jail after admitting terror charges', Northern Echo (21.5.22).
[275] www.counterterrorism.police.uk.
[276] MI5 website (14.7.21).
[277] For the purposes of Prevent referrals, the majority of those aged under 15 and 15-20 have MUU ideologies: Home Office' Individuals referred to and supported through the Prevent Programme, England and Wales, April 2020 to March 2021: data tables', Table 9. There is uncertainty about what practitioners mean by MUU, and it is possible that MUU encompasses perfectly coherent but unfamiliar ideologies.
[278] Care is needed that scepticism about ideological commitment is applied evenly. It cannot be excluded that practitioners from same cultural background as the subject will find it easier, or be more inclined, particularly in the case of children, to find reasons other than terrorist ideology at work.

- Each arrest may be the culmination of, and will certainly lead to, investigation involving the commitment of significant resources.
- Even if they are quickly released, the consequences of a CT arrest are likely to be high significant for the child and their family. Schooling is often brought to an abrupt end through exclusion.
- Where a child has committed serious terrorism offences, the effect of prosecution and conviction[279] is profound.

5.14. Ultimately, the crude but intuitive response is legitimate: something appears to be going profoundly wrong when children are being arrested for terrorism. For children arrested on account of their online behaviour:

- It is doubtful that all of them are really terrorists in any meaningful sense[280].
- At a broader level, there is little public impact or terrorising of the public. Merely committing terrorism offences such as encouragement or dissemination is different from committing real world acts of violence; if prosecuted their cases are usually subject to some sort of reporting restrictions, and little may ever be known about their activities. But for the fact that CT Police cannot ignore the greater risk, it could be characterised a private dance between CT Police and misguided children.

Mental health and Neurodiversity[281]

5.15. No figures exist for neurodivergent individuals or those with diagnosed poor mental health who have been arrested by CT Police in 2021.

5.16. Reports of children arrested in 2021 included: in May, an autistic boy from Merseyside arrested for online terrorist threats[282]; in June, a vulnerable 15-year-old

[279] The rate of conviction is very high for those charged with terrorism offences: Table A-A.06c.
[280] Hall, J., 'Keyboard Warriors or International Terrorists?', speech to Chatham House (14.7.22).
[281] Autism is not same as having poor mental health although autistic people frequently suffer from poor mental health: Harper, G., Smith, E., Simonoff, E., Cawley, L., Maxwell-Scott, C., Davie, M., 'Children and Youth People's Mental Health', Autistica (March 2019); Harper, G., Smith, E., Simonoff, E., Hill, L., Johnson, S., Davidson, I., 'Adult Mental Health', Autistica (March 2019).
[282] " 'Terror Threat' boy spared custody over synagogue bomb Twitter post" (BBC, 27.4.22).

girl from Derbyshire who was later found that to have been groomed and sexually exploited[283]; in June, an autistic 17-year old from Wearside[284].

5.17. Amongst those sentenced in 2021 was 17-year old Paul Dunleavy, described by the judge as having "personality and developmental issues stemming from his abnormal childhood", and who committed terrorism offences as a 13-year old[285]. In December 2021, Feras Al Jayoosi was sentence for displaying his support of Hamas and Islamic Jihad in a Jewish area of North London: the judge found that his autism and Asperger's reduced his culpability[286]. There is a high incidence of poor mental health amongst Prevent referrals: in August 2021, it was reported that the figure was 70%[287].

5.18. Evidence to the Intelligence and Security Committee of Parliament from CT Police and Home Office officials was to the effect that there appeared to be a link between Extreme Right Wing Terrorism and autism[288].

5.19. My own conversations with CT Police units throughout Great Britain, and other practitioners within the CT system, indicate that poor mental health and/or neurodivergence, particularly but not only amongst children, has, within a short period of time, become a major factor in their caseload. Vulnerability Support Hubs, first piloted in 2016 with funding from the NHS, Home Office and CT Police[289], reflect police perception that practical support is needed on this aspect[290].

5.20. Significantly for this report on terrorism online, Ministry of Justice-commissioned research[291] on convicted terrorists who had risk assessments carried

[283] 'Terrorism charges against Derbyshire schoolgirl are dropped', Derbyshire Live (31.1.22). There were strong indications of poor mental health in her case. She killed herself in 2022.
[284] Subsequently tried as an adult (Luke Skelton): the case is currently ongoing.
[285] 'UK's youngest terror offender walks free from court after recruiting for neo-Nazi group' (Independent, 8.2.15).
[286] 'Man who wore T-shirts backing terror groups sentenced' (BBC, 17.12.21).
[287] 'Up to 70% of people referred to Prevent may have mental health issues' (Guardian, 9.8.21).
[288] ISC, 'Extreme Right Wing Terrorism', supra, at paras 85-86.
[289] Vulnerability Support Hubs are described in this critical article by Aked, H., Younis, T. and Heath-Kelly, C., 'Racism, mental health and pre-crime policing — the ethics of Vulnerability Support Hubs', Medact, London, 2021.
[290] The need to deal with poor mental health is obviously not unique to CT Police: see for example, HM Inspectorate of Constabulary and Fire & Rescue Services, 'Policing and Mental Health: Picking Up the Pieces' (November 2018); Ministry of Justice, 'A Response to the Criminal Justice Joint Inspection: Neurodiversity in the Criminal Justice System, A Review of Evidence', Action Plan (30.6.22).
[291] Kenyon, J., Binder, J. F., & Baker-Beall, C., 'Online radicalization: Profile and risk analysis of individuals convicted of extremist offences' (2022) *Legal and Criminological Psychology*, 00, 1– 17.

out between 2010 and 2017 has revealed a link between poor mental health or personality disorder, and how an individual was radicalised.

- Those who primarily radicalized online were 6.27 times more likely to have a strongly present rating for the presence of mental illness/personality disorder than those who primarily radicalized offline, and they were 4.43 times more likely to have a strongly present rating for the presence of mental illness/personality disorder than those radicalized through both online and offline influences.
- Those more vulnerable to online radicalization are younger males and females, who are typically socially isolated, with a limited (violent) offending history and show a greater likelihood of suffering from mental illness or personality disorder.

5.21. Further research by the same authors included risk assessments carried out in the period 2018 to 2021[292]. This means in effect that the profiles of all terrorist prisoners in England and Wales since 2010 have been analysed (although terrorists who died, were killed, or evaded capture are by definition excluded). The overall breakdown was: Islamist (72%), Extreme Right Wing (18%) and others (10%).

- Those who were primarily radicalised online were more likely to show a strong presence of mental health issues, neurodivergence or personality disorder/difficulties (42%) compared to those who radicalised primarily offline or in a hybrid manner. Although co-morbidity was often present, the most common factor was autism[293].
- A third of the entire cohort (143 out of 437) was reported as having some mental health issues, neurodivergence or personality disorder/difficulties.

5.22. The phenomenon is almost certainly international[294].

[292] Kenyon, J., Binder, J. F., & Baker-Beall, C., 'The Internet and radicalisation pathways: technological advances, relevance of mental health and role of attackers" (MoJ Analytical Series, 2022).
[293] Appx I, Figure 2.
[294] US Department of Homeland Security, US Secret Service 'Averting Targeted School Violence' (2021) gives (at page 36) a figure of 70% having mental health symptoms at around the time of their mass violence plots.

5.23. There has been general academic consensus for some time that lone actors or self-initiating terrorists are more likely to suffer from poor mental health[295]. The discussion about criminality and mental health is frequently characterised by caution about stigmatising people. The debate about mental health and terrorism goes back a long time and attention is rightly drawn to the need to avoid lazy explanations for terrorism based on psychopathy[296].

5.24. However, it is difficult to conclude that CT Police are arresting individuals, or grading them as riskier, because of poor mental health and neurodivergence. In cases of online terrorism, CT Police are likely to know little about the suspect's characteristics before arrest (and the sensitive nature of CT investigations generally precludes any prior enquiries). It is after arrest, during the investigation and and/or the prosecution, that these factors often come to light.

5.25. Fear of causing stigma is a weak basis for relegating this topic. On the contrary, deliberate focus is required.

5.26. Firstly, if individuals with poor mental health and neurodivergent individuals are being arrested (and, as the evidence shows) convicted then CT Police need to be mindful of the impact of arrest and prosecution on vulnerable individuals.

5.27. Secondly, understanding the mental health or neurodivergent aspect may assist in earlier identification and diversion of those who might otherwise be arrested as terrorists. It may also improve risk-grading since (as considered below) the cohort of individuals radicalised primarily online who are most associated with neurodivergence and poor mental health appear to be least likely to carry out an attack. That said, the identification of individuals online who pose a sincere violent threat, versus those who simply engage in disingenuous violent online extremist dialogue, is extremely difficult; and the impact of mental ill health or neurodivergence on terrorist risk will vary between individuals.

[295] Gill, P., Corner, E., McKee, A., Hitchen, P., Betley, P., 'What Do Closed Source Data Tell Us About Lone Actor Terrorist Behavior? A Research Note', (2022) Terrorism and Political Violence, 34:1, 113-130.
[296] Corner, E., et al., 'Reviewing the links between violent extremism and personality, personality disorders, and psychopathy' (2021) Journal of Forensic Psychiatry & Psychology. Studies also suggest higher rates than normal of psychiatric problems amongst jihadists: Copeland, S., Marsden, S., 'The Relationship Between Mental Health Problems and Terrorism', CREST (2020).

5.28. Thirdly, CT Police need to be alert to any possibility that vulnerable individuals are being targeted for recruitment.

5.29. Fourthly, a point that applies equally to TPIMS (see Chapter 8), CT Police need to consider what risk management and risk reduction look like for a wider range of individuals: a lonely neurodivergent individual may be more effectively supported by practical mentoring and diary-filling by an autism specialist than mentoring from a specialist in terrorist ideologies[297].

5.30. Fifthly, a higher incidence of poor mental health or neurodivergence amongst those who are primarily radicalised online may be relevant to the regulation of online safety and online terrorism content[298].

Online Terrorism: Risk and Arrest

5.31. It is reasonable to ask, when CT Police arrest a teenager for their online behaviour, whether anything could have been done to intervene earlier?

5.32. The answer is the problem of attribution. In the online world, the timescale between identifying the individual and needing to arrest may be very short. Whether to arrest is informed by an assessment, principally, of the risk to public safety. Even a known individual who has been referred to Prevent may have a secret and anonymous online life, accounting for some of the arrests of individuals going through the Channel process.

5.33. As ever, judging whether online activity may lead to physical violence is exceptionally difficult, and there is often room for uncertainty about what an individual is up to – in real life and in other parts of their digital life (for example, on encrypted channels). Executive action in the form of arrest may be needed to rule out risk.

5.34. Uncertainty is compounded by young people's frequent "obsessive interest in weaponry" where it is unclear if it is linked to terrorist intent; and "always, always, the online environment" where it requires "new expertise, new sources, new methods" to

[297] The same point can be made for Prevent.
[298] In BBC Three, 'Inside the Secret World of Incels' (14.7.19), Dr Kaitlyn Regehr correctly observes that there is insufficient discussion around mental health implications of our technological culture.

identify threat amongst the "thousands exchanging hate-filled rhetoric or claiming violent intentions to each other in extremist echo chambers"[299].

- It is notable that the last three successful ERWT attacks were carried out, in 2016, 2017 and 2019, by older males who did not demonstrate high levels of technological awareness [300], whereas suspect internet activity, again according to MI5, was "often just online espousal of violent views without any real world accompanying activity"[301].
- This is not to exclude the possibility that children can direct terrorist attacks by others, exemplified by the case of the 14-year old RXG and the Anzac Day Plot[302].
- This uncertainty may ultimately be mitigated by years of experience: CT Police and MI5 have had much more experience in dealing with other sources of terrorist risk.
- To some extent, as with intelligence on school shootings, CT Police are having to step in to deal with a risk that no other part of the policing system is designed for.

5.35. The MoJ-commissioned research for the period 2010-2021 that I have already referred to[303] found that those who were primarily radicalised online were more likely to have committed a non-violent index offence (84%), least likely to have held the role of attacker (16%) and showed comparatively low levels of terrorist recidivism.

- For this group, only a minority of attack-plots moved from the planning to the execution stage (29%) with 18% completed.

[299] DG of MI5 threat assessment 2021, supra. Practitioners have spoken to me of "teenage edgelords" and "dark fandom".
[300] Stanwell stabbing, March 2019 (Vincent Fuller, aged 50); Finsbury Park mosque attack, June 2017 (Darren Osborne, aged 47) and murder of Jo Cox, June 2016 (Thomas Mair, aged 52): a point made by the ISC, Extreme Right Wing Terrorism' supra, at para 90. Another interesting point is that, according to John Jupp, J., 'From Spiral to Stasis? United Kingdom Counter- Terrorism Legislation and Extreme Right-Wing Terrorism', (2022) Studies in Conflict & Terrorism, since 2007 13 individuals motivated by ERWT ideology have been convicted of section 5 attack-planning, but were all apparently acting alone.
[301] ISC, 'Extreme Right Wing Terrorism', supra, at page 63. It is also possible that those who are principally operating online have less capability to go through with an attack, or have less operational security and are therefore more easily thwarted, than those who operate predominantly offline.
[302] See RXG v Ministry of Justice [2019] EWHC 2026 (QB) at paras 2-3.
[303] Kenyon, J., Binder, J. F., & Baker-Beall, C., MoJ Analytical Series 2022.

- It appears that these individuals are most likely to leave clues about their intent meaning greater opportunities for disruption (thus "…counter[ing] the popular notion that the Internet helps create an undetectable threat of lone actors").
- The group also had the lowest levels of engagement, intent, and capability. By contrast to purely online interaction, offline contacts played an important role in deepening an extremist identity and hardening resolve to carry out an attack.

5.36. The report draws two striking conclusions: firstly, that those who were primarily radicalised online present a lower level of risk overall; secondly, since this group is now dominant amongst terrorist offenders, it may (at least in the view of the authors of the report) provide evidence that the overall threat of serious and significant harm from terrorist offending in England and Wales is starting to diminish.

5.37. Some caveats are needed before the further conclusion that online terrorism is not really a real world threat.

- This is because, at a practical level, it is not straightforward to determine whether a convicted terrorist offender's conduct is limited to the online sphere.
- Firstly, the offence for which the individual has been convicted may not fully describe their conduct: for example, an individual convicted of possessing information useful to a terrorist may also have shown an interest in carrying out hostile reconnaissance of targets.
- Secondly, some offences committed purely online will (such as purchasing precursor chemical from an online retailer) or may (such as encouraging a third person to carry out an attack) have physical consequences in the real world unless disrupted.
- Nonetheless, it is likely that there is a section of arrested individuals of whom it can be said that they are just keyboard warriors.

Detention under section 41

5.38. For the 32 people arrested under section 41, 31 applications were made and granted for warrants of further detention[304].

[304] Table A-A.13a. There can be multiple applications for one person, so these figures do not necessarily mean that 31 out of 32 people were subject to warrants of further detention.

5.39. Warrants are decided on by specialist magistrates (acting as 'judicial officers') under Schedule 8, who are required to consider the necessity for further detention (for example, for questioning under caution) and the diligence and expedition of the investigation[305].

5.40. 14 days is the maximum period of detention allowed: towards the top end, 6 were detained for between 11-13 days; the most common period of detention was 5 days, followed by one day[306].

5.41. All requests for access to a solicitor (31) were allowed immediately[307].

Charge rate

5.42. In 2021, terrorism-related arrests led to the lowest number of charges ever (57, down from 73 in 2020), whilst the highest number ever were bailed to return or released under investigation (85, up from 33 in 2020).

- The practice of bailing to return or releasing under investigation in a terrorism investigation is a relatively new one but the use of the tactic is accelerating: 85 is more than all previous years put together[308].
- This suggests an overall lessening in the risk profile of those arrested because otherwise, they would most likely have been arrested under section 41 and detained until a charge could be brought (or not).

5.43. Of the 32 arrested in 2021 under section 41, 22 (up from 12 in 2020) were charged. Half of these individuals were detained under Schedule 8 for between 5 and 6 days pre-charge[309].

5.44. The balance in 2021, as in 2020 but more so than in preceding years, was for charges under terrorism legislation (49 out of a total of 57) rather than under non-terrorism legislation (murder, explosives, firearms)[310].

[305] Para 32.
[306] Table A-A.02.
[307] Table A-A.13b.
[308] Table A-A.03.
[309] Table A-A.02.
[310] Table A-A.04.

5.45. Since terrorism legislation is characterised by pre-cursor liability this suggests that the vast majority of people arrested in 2021 had not taken concrete steps towards an attack, although there were 3 charges of attack planning under section 5 Terrorism Act 2006 (the joint lowest figure for this offence)[311].

5.46. As with 2020, the leading terrorism offences charged are possession of information likely to be useful to a terrorist under section 58 Terrorism Act 2000 and dissemination of terrorist publications under section 2 Terrorism Act 2006[312]. These are typical online terrorism offences.

5.47. Interestingly, there is an increasing use of section 57 Terrorism Act 2000 (6, the most since 2008) which penalises possession of an article with terrorist intent. Several years ago it appeared that section 57 might be becoming redundant[313]. As I discuss in Chapter 7, it is desirable that the CPS do charge this offence where they can in preference to section 58 Terrorism Act 2000, because the latter does not require any terrorist intent, and in general individuals should be held accountable for what they intend to do.

[311] Table A-A.05a.
[312] Ibid.
[313] Hill, M., 'Ensuring legislation effectively mitigates the increasing terror threat' (16.1.18).

6. STOPPING THE TRAVELLING PUBLIC

Generally

6.1. The power to examine people travelling through ports, and at the Northern Ireland Border, is found in Schedule 7 Terrorism Act 2000. It is a no-suspicion power exercised by CT Borders Policing.

6.2. From the point of view of a member of the public, its principal impacts when exercised are:

- Questioning, with an obligation to cooperate on pain of committing an offence. There is no right to silence, but answers cannot be used in any subsequent criminal prosecution.
- Search, most notably copying of computers or mobile phone devices.
- Taking of biometrics.
- Detention for up to 6 hours, including automatic detention for any examination over one hour.
- Inconvenience and possible disruption to travel plans.

6.3. From the point of view of CT Police and MI5, the interactions made possible by Schedule 7 are hugely valued sources of intelligence, and occasionally evidence. The value of border questioning backed by intrusive powers is well-illustrated by reference to the period 2013-17, when British citizens and residents sought to travel through UK airports and seaports to Islamic State-controlled territories.

6.4. This strong power has attracted particular attention in my annual reports, and those of my predecessors. Questions about whether it continues to strike the right balance between security and freedom can only be judged by attention to how the power is exercised from year to year.

6.5. I am pleased to report that the Schedule 7 power is responsibly exercised and, importantly from the point of view safeguards and rights, is the subject of strong internal data-driven scrutiny by CT Police. This scrutiny has however identified inconsistencies between different parts of the UK which indicate that improvements are possible.

6.6. The government and CT Police have accepted all my recommendations concerning Schedule 7 in last year's annual report.

6.7. Complaints data about the exercise of Schedule 7 are to be routinely captured from all UK police forces. This should give CT Police (and me) a jumping-off point to consider whether additional thematic issues require attention. Although Schedule 7 has become less controversial over recent years[314], probably resulting from the dramatic decline in its use which suggests better targeting, vigilance about any no-suspicion power remains essential.

6.8. CT Borders Policing recognise that there are regional differences in the way that Schedule 7 is exercised. This is likely to reflect, in part, the fact that Schedule 7 was once the purview of Special Branch Units reporting to 43 different Chief Constables. It certainly reflects the different infrastructure available at ports and seaports. Matters such as office-space, or the distance between the front-line officers and their equipment, are relevant to how decisions are made on the ground.

6.9. Work is being done to ensure greater consistency of language and internal organisation, with a continuing focus on the utility of Schedule 7. The latter point is important. As shown by the demise of the no-suspicion stop and search power under section 44 Terrorism Act 2000, no terrorism power is intrinsically necessary – once it is no longer useful, it loses its reason to exist.

6.10. I will report next year on the new power of examination applicable to irregular – principally but not only 'small boat' – arrivals. The new power was inserted into Schedule 7 by the Nationality and Borders Act 2022 and a new Code of Practice was approved in July 2022[315].

Examinations

[314] Cf the generally positive findings in Wood, S., & Gardiner, S., 'Policing U.K. Airports and Schedule 7 of the Terrorism Act 2000: The Young Passengers' Perception of Security Measures', (2021) 33 Terrorism and Political Violence 1621. A procedural justice approach was found to be important in this Australian study

[315] My response to the consultation on the new Code of Practice is at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2022/04/220401-Response-Sched-7-Code-Consultation.pdf. It addressed the question of how the right against self-incrimination should be protected.

6.11. In 2021 there was yet another fall in the number of those examined in Great Britain: 2,495 down from 3,315 in 2020. For comparison, in 2012 the figure was 60,127[316]. A full year of travel without Covid-19 restrictions is needed before trend analysis is possible.

6.12. 4 of these examinations involved a strip search[317].

6.13. There were 139 examinations carried out in Northern Ireland. The total number of examinations carried out at a port when travelling within the UK was 572[318].

Ethnicity of those examined

6.14. There was a broadly similar reduction across all ethnicity categories from 2020, with the result that in 2021 the following were examined (with percentage of total examinations in brackets):

- 406 (16%) White people,
- 113 (5%) people of mixed ethnicity,
- 170 (7%) Black people,
- 643 (26%) Asian people,
- 588 (24%) 'Chinese or Other' people, and
- 575 (23%) cases in which ethnicity was not stated.

6.15. The Home Secretary has accepted my recommendation on increasing the ethnicity categories, increasing the number from 6 to 17 and on disaggregating the 'Chinese or Other' category, which has historically been used to include Arab people. In addition, officials are working on capturing ethnicity data where individuals do not, perfectly understandably, want to define their own ethnicity.

6.16. National CT Policing HQ have also accepted my recommendation to analyse the ethnicity categories for those subject to tasked examinations compared to untasked examinations.

[316] Home Office, Statistics on the operation of police powers under the Terrorism Act 2000 and subsequent legislation, Year to December 2021: Annual Data Tables, Table A-S.03.
[317] Table A-S.03.
[318] Table A-S.04.

- The risk of racial or religious bias must be greatest when CT Borders Policing carry out high discretion stops, based on experience, behavioural analysis, or a sense that something is worthy of examination. In some locations, particularly sea-ports, examining officers may have little information to go on before they must decide whether to exercise the power.
- The ethnic profile of the overall number of untasked examinations ought to bear some relationship to be the ethnic profile of current Subjects of Interest, the threat picture (for example, terrorist developments in the Sahel), factoring in the likelihood of international or intra-UK travel[319].

6.17. The importance of avoiding discrimination in the use of Schedule 7 was emphasized in a recent decision of the High Court[320]. A conviction for failing to cooperate could only be sustained if the exercise of the power was lawful in the first place and this meant that in some cases the prosecution would have to prove beyond reasonable doubt that no unlawful discrimination had occurred[321].

- In that case, the examining officer admitted that the appellant's political views (a protected ground) were a factor in his decision to examine him.
- However, the High Court held that it was legitimate for the officer to question the appellant about his political beliefs to determine whether he was a terrorist, and therefore there was no unlawful discrimination at work.

Detention

6.18. The total number of detentions in 2021 in Great Britain was 1,117 (out of 2,495 examinations)[322]. The reduction of 6% from detentions in 2020 (1,191) was smaller than the 25% reduction in the total number of examinations.

6.19. In the United Kingdom total detentions amounted to 1149 (out of a total of 2631 examinations). 34 detentions occurred in Northern Ireland[323].

[319] So if there was a domestic terrorist group whose members or affiliates rarely travelled abroad, one would not expect to see their members reflected in ethnicity figures.
[320] Cifci v Crown Prosecution Service [2022] EWHC 1676 (Admin), concerning a member of the Kurdistan National Congress.
[321] At para 32.
[322] Table A-S.03.
[323] Table A-S.04.

6.20. Year on year, the percentage of those who go on to be detained has mounted. Even allowing for the requirement for detention in any case of examination beyond one hour[324], which means that no comparison can be made with figures more than 7 years ago, the proportion has increased year-on-year. Soon it is likely that over half will be detained. This is likely to be a consequence of better targeting: if CT Borders Policing are more convinced at the outset that they need to examine, the more likely it is that they will require longer to examine the individual.

6.21. In my first annual report I questioned the appropriateness of detention after one hour[325]. In response the Home Office led a review of detention across CT Police which concluded, based on internal surveys, that detention was not automatic but followed from a separate decision point during which the necessity and proportionality of detention was considered.

6.22. The review identified some operational difficulties in getting solicitors 'airside' to give legal advice, where requested, and that improvements could be made in explaining the process to a detained person. In 4 cases in 2021, an individual had their access to a solicitor deliberately delayed under powers in Schedule 8[326].

6.23. No progress has been made in securing visits to places of Schedule 7 detention in accordance with Article 4 of the Optional Protocol to the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment[327]. This has been chiefly owing to organisational changes within the UK's National Preventive Mechanism, who are responsible for monitoring places of detention.

Ethnicity of those detained

6.24. The ethnicity of those detained (followed by percentage of total detained) is as follows:

- White people: 156 (14%)
- People of mixed ethnicity: 62 (6%)
- Black people: 64 (6%)

[324] Brought in by the Anti-Social Behaviour, Crime and Policing Act 2014.
[325] Terrorism Acts in 2018 at 6.93.
[326] Table A-S.03. The power is in paragraph 7A of Schedule 8.
[327] See Terrorism Acts in 2020 at 6.23.

- Asian people: 292 (26%)
- "Chinese or Other" people: 276 (25%)
- Not stated: 267: (24%).

6.25. The percentages are broadly in line with the equivalent figures for examination: in 2021 a person in one ethnic category who was selected for examination was no more likely to be detained than a person in another ethnic category.

Phone examination

6.26. Schedule 7 permits the search of individuals including their phones[328], meaning that increasingly large amounts of personal data are available to be viewed, copied and retained.

6.27. I have already referred to regional variations in practice. At its best, where facilities allow, tailored automatic searches can be programmed that reduce the time spent examining a phone, and reduce the risk of collateral intrusion by weeding in or out certain files before human review.

Remote Access

6.28. The government has accepted my recommendation that – because of its current limitations – Schedule 7 needs amendment to allow for the proportionate use of remote searching.

6.29. Much information routinely accessible from a mobile phone is held on the cloud, but there are obvious dangers of allowing CT Police unfettered access to all remotely stored data. This would transform the search of a person's phone when they pass through an airport or seaport into a search of all their remote digital storage.

6.30. The issue of investigatory access to remote data is far wider than Schedule 7 (or Schedule 3, the equivalent power to deal with hostile state threats), which explains why the matter remains unresolved. I have considered how the law might be adapted to deal with remote data in detail in Chapter 4 (Investigations).

[328] Para 8 of Schedule 7.

Phone data Retention

6.31. The government accepted last year's recommendations that a new policy on digital data retention, with accompanying amendments to the Schedule 7 Code of Practice, needs to be crafted. It should explain clearly, and accurately[329], how data is retained and how if ever data is destroyed once the need to retain has expired.

6.32. In Chapter 4 (Investigations) I have considered the topic of retention of electronic data in more detail.

Biometrics

6.33. For the purposes of the Terrorism Act 2000 and the Counter-Terrorism Act 2008, biometrics means fingerprints and DNA, excluding more modern biometrics such as facial mapping or gait analysis.

6.34. 2021 is the first year in which statistics on biometrics have been published. In the United Kingdom at least one biometric identifier was taken from 1031 people (out of a total 2631 examined). All but one of these people were detained[330].

6.35. As a result of the Home Office-led detention review, CT Borders Police have agreed to review their ports and borders biometric policy. The purpose is to ensure that a separate proportionate decision to take biometrics, or not, is taken; and that there is no blanket or automatic approach.

6.36. It is good that the need for a refreshed policy has been detected, less good that some examining officers still need to be reminded of the importance of separate decision-making for all the intrusive powers under Schedules 7 and 8.

6.37. In his annual report for 2020-21, the Biometrics Commissioner noted that biometrics taken under Schedule 7 were "invaluable" [331]. The role of the

[329] In Re Gallagher [2020] AC 185, the Supreme Court put it in this way: for an interference to be in accordance with the law, it must past the dual test of accessibility and foreseeability. At the moment, what happens to phone data is neither accessible nor foreseeable.
[330] Table A-S.05.
[331] Commissioner for the Retention and Use of Biometric Material, Annual Report 2020 (2021).

Commissioner[332] has been to review the retention of biometrics, most of which have been taken under Schedule 7, for national security purposes. I consider the position of Interpol-derived biometrics in Chapter 4.

Freight

6.38. In 2021 there were 710 examinations of air freight, and 614 examinations of sea freight. This is an increase for air freight examinations from 2020 (518), but a major decrease for sea freight examinations from 2020 (2314).

Hostile State Activity Powers

6.39. Schedule 3 to the Counter-Terrorism and Border Security Act provides an equivalent regime of no-suspicion examination (and associated powers) for hostile state activity. The Investigatory Powers Commissioner is charged with reporting on the operation of this regime[333].

6.40. There is the possibility, recognised within both Codes of Practice, that a Schedule 7 examination might turn into a Schedule 3 examination, and vice-versa. There has been one case to date of a transition between regimes: this appears to have been very much the exception.

[332] Following a recent consultation, in which the government had proposed transfer to the Information Commissioner, the government has proposed that this post should be abolished and the role transferred to the charge of the Investigatory Powers Commissioner. My response to the consultation is here: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2021/10/Biometrics-Consultation-Response.pdf.
[333] Sched 3, para 62.

7. TERRORISM TRIALS AND SENTENCING

Criminal Cases in 2021

7.1. 2021 witnessed:

- The sentencing of a probationary police officer, Benjamin Hannam, for membership of a proscribed organisation, National Action[334].
- The first terrorism case involving 3-D printed gun parts (Dean Morrice, a neo-Nazi former British army driver, sentenced to a 23-year extended sentence)[335].
- The conviction of Hisham Chaudhary who funded Islamic State with BitCoin[336].
- The Syria-returner Stefan Aristdou, who was convicted of disseminating terrorist publications prior to his travel to join Islamic State/ Da'esh[337]. He had already served a sentence in a Turkish prison for membership of Islamic State.

7.2. The following children (all boys) were convicted of terrorism offences in 2021:

- from Cornwall, arrested July 2019, aged 16 at sentencing, 24-month Youth Rehabilitation Order for being the UK head of the proscribed organisation Feuerkrieg Division[338].
- from Kent, arrested in September 2021, aged 16 at sentencing, 12 month Youth Referral Order for his role in setting up and running 'British Hand', an Extreme Right Wing group[339].
- from Derby, arrested Sept 2020, aged 16 at sentencing (British Hand), 2 year Youth Referral Order for involvement with 'British Hand'[340].
- from Gloucestershire boy, arrested, Dec 2019, 12 months referral order for downloading explosives manuals[341].

---

[334] Sentencing remarks: https://www.judiciary.uk/wp-content/uploads/2022/07/R-v-Hannam-Setencing-Remarks.pdf (last accessed 6.10.22).
[335] 'Police issue warning over terrorist use of 3D-printed guns as UK neo-Nazi jailed' (Lizzie Dearden, Independent, 15.6.21). The sentence comprised 18 years' imprisonment and 5 years of extended licence.
[336] 'Sales consultant guilty of Bitcoin Islamic State terrorism funding' (BBC News, 6.7.21).
[337] 'British man sentenced to 28 months' imprisonment for sharing Daesh beheading videos' (Crown Prosecution Service, 1.10.21).
[338] 'Youngest British terrorist sentenced for neo-Nazi manuals stash' (Crown Prosecution Service, 8.2.21).
[339] 'Derbyshire schoolboy who ran right-wing terror cell avoids jail' (DerbyshireLive, 9.9.21).
[340] Ibid.
[341] 'Gloucestershire boy sentenced for terrorism offences'(Gloucestershire Constabulary, 29.7.21).

- from Newcastle, arrested Oct 2019, sentenced to 12 months intensive referral order, who invited support for the proscribed group National Action[342].

7.3. Matthew Cronjager was 17 at the time of his arrest in Dec 2020. Also involved with 'British Hand', and aged 18 at sentencing, he was sentenced in 2021 to 11 years 4 months detention in a Young Offender Institution for attack-planning and other terrorism offences[343].

7.4. Analysis of the principal offences for which proceedings were brought by the Crown Prosecution Service in 2021[344] reveals the following.

7.5. First, a continuing decline in prosecutions relating to proscribed organisations[345] (2, down from a peak of 12 in 2018), most likely because of the decline in operational activity against the neo-Nazi proscribed group National Action.

7.6. Secondly, a continuing decline in prosecutions for attack planning[346] (2, down from a high of 24 in 2017).

7.7. Thirdly, that the most frequently prosecuted terrorism offences are documentary-type offences which are typical of online activity: collection of information useful to a terrorist[347] (9), dissemination of terrorist publications[348] (9) and encouragement of terrorism (7)[349]. I consider these offences in more detail below.

7.8. Fourthly, as in 2020, a significant number of the number of offences associated with breaching post-release measure[350] and TPIMS (8, compared to 10 in 2020, but compared to 6 in 2019 and zero in 2018).

7.9. Fifthly, one prosecution brought for murder (Ali Harbi Ali, for the murder of Sir David Amess, but not tried until 2022) and one for explosives offences.

---

[342] 'Teen who called himself Hitler sentenced for terror offences' (BBC News, 30.3.21).
[343] Sentencing remarks, HHJ Lucraft QC, Recorder of London, 19.10.21.
[344] Home Office, Statistics on the operation of police powers under the Terrorism Act 2000 and subsequent legislation, Year to December 2021: Annual Data Tables, Table A-C.03.
[345] Sections 11-13 Terrorism Act 2000. It is possible that the one instance of fundraising (sections 15-19) related to a proscribed organisation.
[346] Section 5.
[347] Section 58.
[348] Section 2 Terrorism Act 2006.
[349] Section 1.
[350] Under part 4 Counter-Terrorism Act 2008.

7.10. Once again there was no prosecution for the Designated Area Offence[351] for the simple reason that no area has yet been designated. As I have previously reported, designating the territory of another country as a no-go area, and criminalising those who travel there, is a delicate business.

- The law was passed to counteract the pull of another 'Caliphate' (Islamic State/ Da'esh's former area of control in Syria and Iraq), if it ever came along.
- This perhaps reflects a truth about terrorist offending, that just as terrorist groups come and go (such as Italy's Red Brigade or Germany's Red Army Faction), so modes of terrorist conduct also wane and wax.

Information Offences

7.11. The three most frequent principal offences in 2021 – possession of information likely to be useful to a terrorist, encouragement and dissemination of terrorist publications - are frighteningly easy to commit online[352] and can be committed anywhere in the world[353].

7.12. As with many offences under terrorism legislation, the purpose of these 'information offences' is to allow the authorities to intervene well before any act of terrorist violence is committed.

7.13. It is not necessary that a terrorist attack plan has been formulated. The reasoning is that if fewer individuals are encouraged to terrorism generally, or in possession of information that is likely to be useful to a terrorist generally, then fewer attacks will ultimately happen. For these offences it is not necessary that someone was in fact encouraged to commit an act of terrorism[354] or deployed the useful information.

[351] Contrary to section 38B Terrorism Act 2000.
[352] Section 58 Terrorism Act 2000; sections 1, 2 Terrorism Act 2006.
[353] Section 63A Terrorism Act 2000, section 17 Terrorism Act 2006, noting that extraterritorial jurisdiction for the section 58 offence only applies to UK nationals or residents.
[354] Sections 1(5)(b) and 2(8).

7.14. This reasoning begs the following question: since information offences do not actually hurt anyone, does criminalising this type of conduct in fact prevent terrorist attacks further down the line?[355]

7.15. In 2007 Parliament's Joint Committee on Human Rights, scrutinising the encouragement offence, observed that doing something was different from saying something and that "speech does not naturally reside in the realm of criminality"[356]. The same point may be made about information offences.

7.16. In fact, a nexus *has* frequently been found between information offences and terrorist attacks. The offence of collecting or possession information likely to be useful to a terrorist was typically (and justifiably) applied, in Northern Ireland, to individuals who sat outside police stations noting number plates, with a view to tracking down and assassinating police officers. Numerous attacks have been carried out by individuals inspired by Al Muhajiroun's words[357].

7.17. But the ease of committing these offences online begs the question whether this nexus holds good.

- These offences are practically easy because there are already so many terrorist publications or terrorist manuals in circulation online, which can be downloaded or forwarded[358].
- These offences appear to be psychologically easy to commit because of the disinhibiting effect that leads people, especially when they are posting anonymously, to communicate things online when they would not do so offline; and because a willing and engaged audience can always be found.
- This can be tested by considering the counter-factual: absent the internet, how easy would it be to obtain a bomb manual? Where would you go? Who would you have to meet? If you wanted to encourage someone else to commit an act

[355] Considered by Zekulin, M., 'From Inspire to Rumiyah: does instructional content in online jihadist magazines lead to attacks?', (2021) Behavioral Sciences of Terrorism and Political Aggression, 13:2, 115-141. The answer is that there is no straightforward relationship between material appearing and attacks being carried out.
[356] Joint Committee on Human Rights, The Council of Europe Convention on the Prevention of Terrorism, First Report of Session 2006–07, paragraph 9.
[357] See Terrorism Acts in 2020 at 8.14.
[358] OFCOM, 'Online Nation' (9.6.21), records that 9% of social video platform users had been exposed to 'radicalisation or terrorism' within the last 3 months.

of terrorism, how would you go about finding a potential audience? How would you avoid being reported to the police?

7.18. I have already examined in Chapter 5 (Arrest), the exquisite difficulties facing investigators when they encounter information offences in assessing whether the individual poses a genuine risk.

7.19. Because of this uncertainty, investigators and prosecutors need to tread with care before deploying the information offences, each of which now carries – since the enactment of the Counter-Terrorism and Borders Security Act 2019 – a sentence of up to 15 years' imprisonment, and, being terrorism offences, carry a long tail of legal (post-release monitoring, possible exclusion from legal aid[359]) and potential practical (de-banking, travel problems) consequences. Non-terrorism offences will sometimes fit the bill[360].

7.20. In 2021, the section 58 offence (information likely to be useful to a terrorist) formed part of the prosecution of the following neo-Nazi adherents:

- the co-founder of National Action, Ben Raymond. He had Norwegian terrorist Anders Brievik's manifesto and a guide to homemade detonators[361].
- In Scotland, the socially-isolated Sam Imrie, who threatened to burn down a mosque and had copies of manifestos by New Zealand attacker Brenton Tarrant and Anders Brievik[362].
- Ben John, who had possession of the Anarchist's Cookbook[363].

7.21. My conclusion in last year's annual report was that the justification for the section 58 offence had not fallen away; that it remained at the outer edges of legitimacy; but that it continued to be deployed sensitively because (as in the three cases listed above) there was usually evidence of terrorist intent or terrorist sympathy[364].

[359] If Part 4 of the National Security Bill is enacted in its current form.
[360] For example, DPP v Kingsley Anthony Smith [2017] EWHC 359 (Admin), a prosecution under the Communications Act 2003 for posting "Kill the Kuffar Allahu Akhbar" to the defendant's Google+ profile page for public viewing. See also the offences listed in CPS, 'Social Media – Guidelines on prosecuting cases involving communications sent via social media' (21.8.18).
[361] 'National Action: Ben Raymond jailed for eight years' (BBC News, 3.12.21).
[362] Imrie's case is considered in Chapter 10.
[363] John's sentence was found to be unduly lenient in R v John [2022] EWCA Crim 54.
[364] Terrorism Acts in 2020 at 7.23-7.45.

7.22. The acquittal in a recent Scottish case[365] suggests that juries may baulk at convicted individuals with the section 58 offence unless satisfied that the individual is a terrorist or terrorism-aligned.

- No challenge was made to the elements of the section 58 offence having been established by the prosecution.
- However, the defendant had autism and an obsessive interest in experimenting with explosives and collecting material online.

7.23. Although less often prosecuted[366], the offence contrary to section 57 Terrorism Act 2000 (possession of article with terrorist intent) can also be an information offence, since it can apply to documents held with the intention of inducing acts of terrorism[367]. This is an information offence that is more justifiable in the online context: although the act of acquiring information is easily committed, a terrorist intention is required before criminal liability can be imposed under this section[368].

7.24. It is comforting to think that greater digital literacy, and awareness of the risk of terrorist arrest, will lead to fewer information offences. However, children and young people tend not to think about the longer-term impacts of offending[369]. It is also far easier to call for parents to exercise greater oversight of their children's digital lives, than to achieve it. These offences are here to stay.

Online Encouragement

7.25. Assuming a terrorist prosecution is the correct response, a technical, but important, issue arises about the scope of the encouragement offence. It arises because of the novel way in which communications operate online.

Online Context

[365] R v Richard Smith. 'Man cleared of terrorism and explosives offences in Aberdeen' (BBC News, 14.6.22).
[366] It was charged 6 times in 2021: Table A-A.05a.
[367] R. v. Zafar, Butt, Iqbal, Raja and Malik [2008] EWCA Crim 184, at para 31.
[368] Strictly speaking, section 57 does not require proof of a terrorist purpose. However, it is a defence that the article was not held with such a purpose. This is an important distinction between the seriousness of section 57 and section 58 offences: see for example, Secretary of State for the Home Department v NF [2021] EWCA Civ 17 at para 36.
[369] College of Policing, 'Scared Straight programmes' (19.2.15) found that children and young people who participated in prison visits intended to scare them from reoffending were *more* likely to reoffend in future.

7.26. It is extraordinarily easy to create privacy online, but it is not exactly privacy as it exists in real life.

- You can limit viewers of your private YouTube account to 50 invitees – these could be your friends or family or complete strangers.
- You can set your privacy settings on Facebook to friends or friends of friends, and only they can see what you post. This may result in sharing information with people you have never met.
- You can be accepted by a site administrator into a 'closed' group, potentially containing many thousands of other users[370], allowing you to communicate instantaneously and securely but to the exclusion of the rest of the world. These individuals are unlikely to be using their real names and may be anywhere in the world,

7.27. All this activity may be backed up by powerful encryption – chosen or (in some cases, for example, WhatsApp) applied by default.

7.28. In the online context, prosecutors have struggled with the question of whether communicating within a 'closed group' amounts to publication to members of the public. This is a factor that has inhibited the bringing of prosecutions for certain forms of online conduct. The question therefore arises whether the section 1 offence continues to be fit for purpose in the online age.

Criminalising Encouragement

7.29. Legislation to criminalise the encouragement of terrorism was already in contemplation before the 7/7 attacks on the London Transport System in 2005 but taken through Parliament in the immediate aftermath.

7.30. The immediate reason for creating the offence was to comply with the Council of Europe Convention on the Prevention of Terrorism 2005, article 5 of which required states to criminalise "public provocation" to commit a terrorist offence "with the intent

[370] Telegram groups accept up to 200,000.

to incite the commission of a terrorist offence" where such conduct "causes a danger that one or more such offences may be committed"[371].

7.31. The Terrorism Bill 2005 went further by also establishing liability for recklessness[372]; but the government was clear that the scope – publication to "members of the public" rather than simply "persons" – should go no further. It was not thought appropriate for this offence "to target private communications"[373].

7.32. At the time, Parliament does not appear to have viewed the encouragement offence in the same category as more traditional terrorism offences: it did not amend the definition of "terrorist" to include a person who commits an encouragement offence[374] and specifically exempted the encouragement offence from the scope of a terrorist investigation[375].

Section 1

7.33. Section 1 applies to a statement "published" to "members of the public"[376]. The key characteristic of the statement is that that it must be reasonably understood as an encouragement or inducement[377] to particular or general[378] acts of terrorism, to be judged from all the circumstances[379].

7.34. The conduct element of the offence is the publication of such a statement[380], which may be of any description including a communication without words consisting

[371] The requirement that there should be intent, and a danger of offences, were deliberate limitations to the scope of the offence: Explanatory Report to Convention at para 39.
[372] The Joint Committee on Human Rights, supra, thought that intention was a necessary limiting factor for any speech offence; MacDonald, S., Lorenzo-Dus, N., 'Intentional And Performative Persuasion: The Linguistic Basis For Criminalizing The (Direct And Indirect) Encouragement Of Terrorism ', Criminal Law Forum (2020) 31:473–512 consider that encouragement lacks the necessary 'illocutionary force' absent intention.
[373] Hansard (HL) 5.12.05 col 435, Baroness Scotland of Asthal, Home Office Minister.
[374] The definition is in section 40.
[375] Section 32(3) Terrorism Act 2000 exempts section 1 and 2 of the Terrorism Act 2006.
[376] It is likely that (as Baroness Scotland said in Hansard 5 Dec 2005: Column 435) the words "to the public" do not add anything; and were probably added because the structure of the offence requires consideration of the likely impact of the publication on the audience.
[377] Including through glorification: section 1(3).
[378] Section 1(5).
[379] Section 1(4).
[380] Section 1(2)(a).

or sounds or images or both[381].The mental element is either intentional or reckless encouragement[382].

7.35. "Members of the public" has a widened meaning under the Terrorism Act 2006[383]. It means not only any section of the public[384] but applies where the public are present in a private setting, because "public" includes references to:

> "…a meeting or other group of persons which is open to the public (whether unconditionally or on the making of a payment or the satisfaction of other conditions)".

7.36. This is a powerful expansion of what is generally understood by "the public" and has relevance to the issue of closed groups.

Contrast to Section 2

7.37. Whereas section 1 deals with original statements, section 2 deals with the secondary dissemination of "terrorist publications". These are documents, either encouraging or instructional[385], that already exist.

7.38. There are various types of conduct that fall foul of the offence such as distributing or transmitting electronically[386]. The mental element is intentional or reckless encouragement or provision of assistance to commit acts of terrorism[387].

7.39. Unlike section 1:

[381] Section 20(6).
[382] Sections 1(2)(b)(i) and (ii). Recklessness means subjective recklessness or awareness of the risk, and there is a special defence in reckless cases that the statement did not have the defendant's endorsement: section 1(6).
[383] By contrast, no such widened meaning applies to the publication of terrorist organisation images under section 13(1A) Terrorism Act 2000, as inserted by the Counter-Terrorism and Border Security Act 2019.
[384] Section 20(3)(a).
[385] Section 2(3)(4).
[386] Section 2(2).
[387] Section 2(3).

- There is no limitation about the audience – the actual or intended audience need not be members of the public. It applies where the distribution etc is simply to family and friends[388].
- Section 2 does not deal with original statements. It does not criminalise the words as they come out of a person's mouth, or as they are formulated on a keyboard. It only applies to pre-existing publications.

7.40. Any penalising of expression requires justification. But because section 1 applies to *original* statements the values of freedom of expression and of personal development through self-articulation – discussed in detail in Chapter 11 – apply with particular enhancement.

7.41. George Orwell wrote of the effect of inhibiting original words in the Appendix to 'Nineteen Eighty-Four' (1949). The purpose of the stunted official language Newspeak was to make unapproved thoughts unthinkable as well as unsayable:

> "…reduction of vocabulary was regarded as an end in itself, and no word that could be dispensed with was allowed to survive. Newspeak was designed not to extend but to diminish the range of thought, and this purpose was indirectly assisted by cutting the choice of words down to a minimum…The intention was to make speech, and especially speech on any subject not ideologically neutral, as nearly as possible independent of consciousness."

7.42. Bringing a speech offence into the private domain because of the danger that a reasonable third party (not necessarily present in the conversation[389]) might be encouraged to violence would need the strongest justification. Individuals should not be forced to monitor their private conversation against such a risk[390].

"Publish" and "members of the public": Online

[388] As observed by Conway, M., 'Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines', Terrorism and Political Violence (2021), Vol. 33, No. 2, 367-380, terrorist propaganda is inherently public – it is produced and circulated online with the express purpose of wide dissemination.
[389] The question under section 1(1), as amended by the Counter-Terrorism and Border Security Act 2019, is how "a reasonable person" would react to the words, not the actual audience.
[390] As to individuals who encourage terrorism in prison, see Hall, J., 'Terrorism in Prisons'.

7.43. Special provision was made in the Terrorism Act 2006 for online commission of the encouragement offence[391]. For user-generators, publishing a statement includes using an online service provided by others "so as to enable or to facilitate access by the public to the statement"[392].

7.44. This is the provision that the Crown Prosecution Service rely on when prosecuting cases of online encouragement.

- It makes explicit what is also accepted in other areas of criminal liability for online publication[393]: it is not necessary for the prosecution to show that a person did in fact read the statement, merely that the public was provided with access to it.
- The provision does not say that access must be easy. In the online context, it may be that only a limited number of individuals have the technical ability or patience to find a 'join-link' necessary to enter the private group[394].

7.45. When the Law Commission considered juror contempt in the context of online messages, it had in mind the words of the Contempt of Court Act 1981, "addressed to the public at large or any section of the public"[395]. The Commission thought it unlikely that an acceptable statutory language could be found to describe the meaning of "section of the public" in the context of evolving new media, and it was therefore appropriate to allow the law to develop on a case-by-case basis.

- Citing textbooks on contempt[396], it suggested that relevant factors might include the size of the group, the nature and function of the group, the means of control

[391] Explanatory Notes, para 11.
[392] Section 20(4)(c). The words "so as to" import a requirement of deliberateness.
[393] See, for the offence of stirring up racial hatred under section 19(1) Public Order Act 1986, R v Sheppard and Whittle [2010] EWCA Crim 65, at para 34. The Law Commission considered that this also applied to contempt of court: see Law Commission, 'Contempt of Court (1): Juror Misconduct and Internet Publications', HC 860 (2013) at 2.30 to 245.
[394] For the use of join-links to enter Telegram closed groups see Clifford, B., Powell, H., 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosytem on Telegram', George Washington University Programme on Extremism (2019). Laying breadcrumbs for access to suspect material appears to part of the extremist ecosystem: cf. R (Chabloz) v CPS [2019] EWHC 3094 (Admin), a case under section 127 Communications Act 2003, where the defendant posted hyperlink on her public blog, seeking to widen distribution of her own antisemitic material. An individual who follows such links is participating in the internet's marketplace of ideas just as much as if he discovered the content via a search engine.
[395] Section 2(1).
[396] Arlidge, Eady and Smith on Contempt (4th ed 2011) para 4-54; Borrie and Lowe: The Law of Contempt (4th ed 2010) para 4.9.

over access to the group or the communication and the context in which the communication was made[397].

7.46. There is no reason a case-by-case approach should not also apply to the meaning of "public", "section of the public" and "members of the public" within the Terrorism Act 2006. A case-by-case approach applies to the meaning of other constituent elements of criminal offences such as the meaning of "public place" in road traffic offences[398] or firearms offences[399].

7.47. However, for the encouragement offence, the special extended meaning of "public" to include meetings to which the public are admitted, whether for payment or on terms[400], must be reckoned with.

- the Terrorism Act 2006 contemplates that not just a section of the public, but a meeting of the public, with no upper or lower limit of numbers.
- There is no limitation to the terms on which the public may be admitted. They may be admitted on Chatham House rules, on the basis that they use encryption, or on the basis they keep the meeting strictly secret[401].
- It is consistent with "meeting" as defined, that a great degree of control may be exercised over who is admitted by, for example, the group administrators.

7.48. In these circumstances, the fact that the administrator of a neo-Nazi forum requires new members to demonstrate their adherence to Seige culture as a term of admission and deploys strong encryption (the technological equivalent of a locked room), does not disqualify those new members from remaining members of the public at a meeting.

[397] Op cit.
[398] The leading case is the decision of Simon Brown LJ in DPP v Vivier [1991] 4 All E.R. 18, DC ("…do those admitted pass through the screening process for a reason, or on account of some characteristic, personal to themselves? Or are they in truth merely members of the public who are being admitted as such and processed simply so as to make them subject to payment and whatever other conditions the landowner chooses to impose.", at page 24.)
[399] Anderson v Miller (1976) 64 Cr App.R 178.
[400] Section 20(3)(b), supra.
[401] Accordingly, the question of whether those present have a "reasonable expectation of privacy" appears to be immaterial. In any event, the concept exempts criminal communications (Bloomberg v ZXC [2022] UKSC 5 at para 53).

7.49. There is no reported authority on this aspect of the encouragement offence. However, in 2020 Shehroz Iqbal was convicted for posting terrorism encouragement onto a 22-member WhatsApp group[402]. I am informed that the question of whether this counted as encouragement to members of the public was not argued, presumably because the defendant knew nothing if anything of the individuals who had made their way to this group. Arguing that these were not members of the public would no doubt have exposed the defendant to embarrassing cross-examination ("What is @jihadi1234's real name? Where do they live?" etc).

7.50. Should the point be contested, it is foreseeable that caselaw will develop a range of factors to which judges or juries should have regard when deciding whether online publication to a closed group is to members of the public. Whilst there will be circumstances in which no members of the public are present (for example, a family WhatsApp group), there is no reason to consider the existence of a small, closed group is necessarily a bar to prosecuting the encouragement offence.

7.51. For these reasons I do not recommend that the encouragement offence is amended, by removing the limitation that it can only be committed where the audience is members of the public.

- Firstly, any information offence directed at original speech or writing, and particularly one that may be committed recklessly, should be kept within bounds and only extended, if at all, where a strong case can be established. If the concern is closed groups, the current encouragement offence has not been shown to be inadequate.
- Secondly, there are other terrorism offences that may plug perceived gaps[403].
- Thirdly, if an extension is made, albeit for online purposes, it will criminalise what people say at home. Criminalising speech at home is a profound step that should not be taken lightly[404].
- Fourthly, even if a way was found of confining an extension to online communications, it must be questioned whether bringing any more

[402] 'Royal Festival Hall: Shehroz Iqbal jailed for inciting attack' (BBC News, 20.11.20).
[403] Sections 12 (inviting support for a proscribed organisation), 54 (weapons training) Terrorism Act 2000; sections 5 (attack-planning), 6 (weapons training); and inchoate offences under sections 44-6 Serious Crime Act 2007 with respect to a substantive offence.
[404] Hence the controversy over the Hate Crime and Public Order (Scotland) Act 2021: see 'MSPs approve Scotland's controversial hate crime law' (BBC News, 11.3.21). Contrast the dwelling house exemption for stirring up racial hatred under section 18 Public Order Act 1986.

communications into scope of terrorism legislation is desirable. CT Police are already contending with an epidemic of online information offences without, at least at present, a concomitant rise in the level of terrorist violence.

Youth Diversion

7.52. A child's online activity is usually the basis for their real or apparent terrorist risk.

7.53. As I discuss in Chapter 5, the authorities struggle to distinguish between mere noise and true threat, but if a decision to arrest is made, it is frequently the case that evidence of terrorist information offences, and sometimes of plots, will be found on seized devices[405].

7.54. This begs the further question – given evidence of terrorist offending, is prosecution the correct outcome for children?

7.55. Although the 2021 cohort of child arrestees are almost exclusively suspected Extreme Right-Wing Terrorists (19 out of 20 arrests):

- Equivalent solicitude is needed for the interests of children connected to other ideologies.
- Recognising that no two cases are exactly alike, there is a constant need to ensure that mitigating factors such as youth are recognised in offenders from minority as much as majority population groups.

General principles

7.56. Special standards apply to the treatment of children within the criminal justice system. Under the UK-ratified Convention of the Rights of the Child, the treatment of suspected or accused children requires consideration of their best interests (as "a primary consideration") and must be "consistent with the promotion of the child's sense of dignity and worth", taking account the child's age and the desirability of promoting the child's reintegration into society[406].

[405] Section 1, 2 Terrorism Act 2006, section 58 Terrorism Act 2000.
[406] Articles 3(1), 40(1).

7.57. The latter refers to reintegration not simply in the sense of passively complying with the criminal law in future but "assuming a constructive role in society"[407]. In considering the prospects for reintegration allowance must be made for the fact that children are still in a state of development, and their risk profile may well change quickly. It may be said that recent reforms within Part 2 of the Counter-Terrorism and Sentencing Act 2021 do not reflect this difference[408].

7.58. Most recent is the UN Committee on the Rights of the Child comment on online activity which recognises the ability of terrorist groups to recruit children online and states that "…Children accused of criminal offences in that context should be treated primarily as victims but, if charged, the child justice system should apply" [409].

7.59. All this means that authorities are encouraged to consider dealing with children, where appropriate, without recourse to judicial proceedings [410], and keeping deprivation of liberty as a measure of last resort and for the shortest possible time[411]. In the latest review of its Global Counter-Terrorism Strategy, the UN General Assembly reiterated its call for States to "consider alternatives to prosecution and detention"[412].

7.60. A further variation is the need to consider whether – if prosecution is necessary – the case can be adequately dealt with using non-terrorism offences. Being a 'convicted terrorist' is not a status to be wished on children if reasonably avoidable.

- Being a terrorist convict leads to more conservative offender management on release. Restrictions on electronic devices or driving can make it difficult to find a job.

[407] Article 40(1).
[408] For certain terrorist offenders the role of the Parole Board has been abolished, and this applies to both adults and juveniles: I made this point in https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2020/06/Note-1-on-Sentencing-Reforms-1.pdf. Dr James Renwick, Australia's Independent National Security Legislation Monitor made similar points in his 'Report to the Prime Minister: the prosecution and sentencing of children for terrorism', at paras 1.15 to 1.25.
[409] UN Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment' at para 83.
[410] Article 40(3)(b).
[411] Convention on Rights of the Child, Article 37(b).
[412] A/RES/75/291 (2 July 2021) at para 117.

- Being a terrorist convict may – if measures currently before Parliament[413] are enacted – result in further restrictions on them to mark the special disdain with which society views terrorist offending.
- Indeed, being a terrorist suspect will often result in school exclusion[414].

7.61. International standards recognising the special position of children are not out of line with CT Police's current approach. I detect no rush on the part of either CT Police or the Crown Prosecution Service (Counter-Terrorism Division)[415] to see children charged with terrorism offences.

7.62. But even where charging is thought appropriate, sentencing outcomes may be comparatively poor from the perspective of risk management. In the calendar years 2020 and 2021, only one defendant convicted of terrorist offences as a child was eventually sentenced to a term of immediate imprisonment (the case of Matthew Cronjager, sentenced to over 11 years' detention). For those who are detained, the post-release reporting requirements imposed by the Counter-Terrorism Act 2008 are not available for those sentenced under 16[416]; nor are Serious Crime Prevention Orders, increasingly imposed on conviction by the criminal courts, available for children at all[417].

7.63. This is not to say that non-custodial sentences lack value. But their benefit comes some way down the line. For example, a child may ultimately be sentenced to a Youth Rehabilitation Order with a requirement to attend sessions with a therapist or mentor; but during the criminal process leading to conviction or plea of guilty, they will be advised (understandably) to avoid discussing their behaviour for fear of incriminating themselves. This stifles other forms of intervention.

7.64. It is questionable whether the heavy commitment of police resources that are required to fully investigate terrorist offending in these cases is worth it. As well as low

[413] Part 4 National Security Bill. I consider the merit of provisions in https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2022/05/NS-Bill-Pt-3-Note.pdf.
[414] Noting that child terrorism cases often involve elements of school shooting fantasies.
[415] On the public interest in prosecuting a child, special considerations apply including the child's best interests and welfare: Code for Crown Prosecutors, paragraph 4.14(d); see also CPS guidance, 'Youth Offenders' (28.4.00); and references to children in CPS guidance, 'Terrorism: Guidance in relation to the prosecution of individuals involved in terrorism overseas'.
[416] Section 44(a).
[417] Section 6, Serious Crime Act 2007.

levels of detention, CT Police are conscious of evidential stumbling blocks that may arise:

- Jurors may be reluctant to accept that children really mean what they say online.
- Jurors may be reluctant to convict those who they do not regard as really terrorists.
- The Modern Slavery youth defence (considered further, below) may complicate matters of proof.

7.65. Even if CT Police believe they have a good case to charge, the CPS may (acting independently as they must) conclude that there is insufficient evidence or that the public interest does not call for prosecution.

7.66. The result is an increasing number of individuals, investigated and arrested by counter-terrorism police, found with evidence of terrorism offending, whose risks are no longer managed down the conventional route of prosecution and incapacitation through imprisonment.

7.67. This begs the question of what successful diversion from the criminal process, which respects the special position of children but adequately protects the public from terrorist risk, might look like.

Alternatives to Charging

7.68. In general, the police have two options with children who have been arrested for terrorism offending:

- Investigation leading to criminal charge.
- Referral to the 'Channel' component of Prevent.

7.69. Channel can draw in the support of local authorities and health providers, leading to mentoring or other specialised assistance, but it is voluntary.

- There are numerous cases in which individuals referred to Channel continued to offend[418].
- Examples exist of children who say one thing to their Channel Intervention Provider by day, whilst by night, free from any restrictions, they participate in terrorist chatrooms; or who break off their attendance, or refuse to attend mentoring sessions all together.
- Channel does not come with constraining measures such as reporting, tagging or restrictions on internet use which are available within criminal bail. This is a keen worry in cases where the risk either is judged to be potentially high.

7.70. Historically, prosecution and Prevent have been mutually exclusive. At worst this could mean that a child is deprived of support, for example mental health support through Prevent, because they are subject to a criminal investigation.

7.71. On the other hand, it is often only after arrest and search (and examination of seized devices) that the scale of a child's involvement in terrorism be understood. Moreover, it is often only where CT Police have shown their hand through arrest ('gone overt') that it is possible to discuss the child's conduct outside the counter-terrorism system, with schools, doctors or local authorities.

7.72. There is one recent case in which the policy of exclusivity was overridden. Prevent interventions continued after arrest and whilst the child was on bail, leading a decision that prosecution was no longer in the public interest. The risk had been identified and the child had demonstrably changed as a result of effective intervention.

7.73. This required close and trusting work between CT Police and the relevant Local Authority with a degree of creativity to reinterpret standard protocols and take (managed) risks, and a focus on the family circumstances of the child. Some CT Police areas will have greater experience of working (including sharing information) with local authorities and schools than others. I expect that the case study, which I have seen, will be brought to the attention of all CT Police areas.

Gaps

[418] Both Shehroz Iqbal, and Ben John, mentioned above, had been previously referred to Prevent.

7.74. While preparing for this annual report, I have enjoyed frequent and wide-ranging discussions with Senior Investigating Officers (SIOs) who lead terrorist investigations. I have also been part of a police-led working group on the phenomenon of child terror suspects, which aims to pull together a list of options.

7.75. The ideal non-criminal disposal for individuals who are not suitable for Prevent would have the following features.

7.76. Firstly, it would be quick to impose, so as not to lose time in rehabilitating the child through effective interventions.

7.77. Secondly, it would impose conditions, such as flexible restrictions on or control or oversight of internet use[419], backed up by a power of arrest to offer reassurance.

7.78. Thirdly it would impose compulsory and rehabilitative mentoring or attendance arrangements.

7.79. Fourthly, it would not be badged as a counter-terrorism measure, to avoid stigma, and cater for the troubling rise in (non-terrorist) school shooter cases.

7.80. Fifthly, it would last for a significant period (for example, up to 2 years).

7.81. Sixthly, it could be imposed whether or not the child consented to it[420].

7.82. Seventhly, it would not result in a complicated disclosure exercise requiring CT Police to take steps to protect sensitive information.

- Whilst CT Police and MI5 are confident in the disclosure process for criminal proceedings, the same is less true in civil proceedings.

[419] Restrictions on internet use are available in police or court bail; licence conditions for release offenders; TPIMs, SCPOs (and Sexual Offences Prevention Orders, see for example R v Smith and others [2011] EWCA Crim 1772), and under the Mental Capacity Act 2005 (for example, Re: A (Capacity: Social Media and Internet Use: Best Interests) [2019] EWCOP 2).

[420] Whilst it is said that consent is "essential (as a matter of principle and for the measure to be effective)" (*General comment No. 24 (2019) on children's rights in the child justice system*, *op. cit.*, paras. 15-8), this may require qualification where the stakes are as high as they are in terrorism cases.

- It is likely that this consideration is behind the fact that, despite amendments to make them more readily available for counterterrorism purposes[421], no SCPO has been applied for in the absence of a conviction.

7.83. Looking at existing non-prosecution measures:

- Youth conditional cautions [422] do not obviate the need for a criminal investigation because there must be a realistic prospect of conviction followed by an admission by the offender[423]. Although breach may result in arrest, the sanction is re-starting the underlying proceedings for the offence that led to the conditional caution[424]. Deferred prosecutions ('Outcome 22'[425]) suffer from this second flaw.
- TPIMs, although strictly speaking available, were not created with children in mind. They require significant preparation to obtain and are resource-intensive to monitor.
- Serious Crime Prevention Orders are not available for children[426].
- Injunctions under the Anti-social Behaviour, Crime and Policing Act 2014 are only available in cases of anti-social behaviour which means conduct that has caused, or is likely to cause, harassment, alarm or distress to any person[427]. This is unlikely to apply where terrorist information is shared consensually on extreme channels.

7.84. Other civil measures may be available because of the circumstances of an offender (rather than his feared terrorist offending) but are either limited to adults or not a realistic option[428].

[421] Section 14 Counter-Terrorism and Border Security Act 2007; section 43 Counter-Terrorism and Sentencing Act 2021.
[422] Section 66A Crime and Disorder Act 1998.
[423] Section 66B. See also Ministry of Justice, Code of Practice for Youth Conditional Cautions.
[424] Section 66E.
[425] National Police Chiefs' Council, 'Outcome 22 – NPCC Briefing note (v1 March 2019)'.
[426] Section 6 Serious Crime Act 2007.
[427] Sections 1, 2(1).
[428] For example, Domestic Violence Protection Notices under the Crime and Security Act 2010 are only available in cases of domestic violence and only extend to 28 days; Violent Offender Orders under the Criminal Justice and Immigration Act 2008 are only available for adults; Gang Related Violence Injunctions under the Policing and Crime Act 2009 are not relevant to lonely online offenders; Knife Crime Prevention Orders under the Offensive Weapons Act 2019 require previous possession of a knife in a public place or school premises; and so on.

7.85. By way of comparison, Canada has made use of its terrorism peace bonds for children[429] and adults[430] (including some seriously risky individuals[431]). These orders may be made where there are reasonable grounds to fear that another person may commit a terrorism offence and last for up to 12 months[432]. Although they may be imposed without consent, I am informed they are generally consensual and sometimes imposed on "couch jihadis" – Canada's version of keyboard warriors. They provide for a range of conditions to be imposed, including treatment and tagging.

7.86. Because a working group currently exists, and because it is possible that existing measures are – contrary to my discussions CT Police and my analysis – adequate in a sufficient number of cases I hesitate to make a positive recommendation about a new power.

7.87. In addition, I am wary of suggesting a measure that, owing to disclosure fears, would be resisted by CT Police where sensitive intelligence has been obtained by investigators (as is generally the case in CT investigations). This seems to rule out the use of any measure in contested cases.

7.88. The most I can do is suggest a potential new model and **recommend** that the Secretary of State and CT Police carry out an exercise to consider whether such a model would be a useful addition. Under this model, to be available for children only:

- The measure would take the form of a statutory court-imposed injunction[433], enabling the imposition of conditions, backed up by arrest and penal sanction for breach[434].
- The types of measures would include positive interventions (e.g. mandated attendance at sessions with an intervention provider) and restrictions (e.g. around phone or device usage).

[429] 'Ontario and Quebec youths placed under terrorism peace bonds' (True North, 26.1.22).
[430] 'Crown seeks terrorism peace bond in Calgary after Canadian mother freed from ISIS detention camp' (CBC News, 25.11.21).
[431] 'Canada extremist Aaron Driver 'was planning attack' (BBC News, 12.8.16). Driver blew himself up whilst on a terrorism peace bond.
[432] Criminal Code 810.011. 5 years maximum in a case of previous terrorism offending as in the case of Kevin Omar Mohamed, 'Terrorism peace bond placed on Ontario man for four years' (Global News, 4.8.21).
[433] As under the Anti-social Behaviour, Crime and Policing Act 2014.
[434] See Schedule 2 for the options available to the sentencing court in the case of children who breach injunctions under the 2014 Act.

- The statutory threshold would be the existence of terrorism material[435] where, owing to the presence of that material, there were reasonable grounds to suspect that the individual would be drawn into using or encouraging acts of violence.
- It would not be badged as a counter-terrorism measure and would be suitable for those who had been drawn into school shooting fantasies, as well as those who (if prosecuted) might be considered to have a terrorist mindset.
- Any application would require certification at chief officer level that the application was appropriate having regard to the child's age and welfare, and the risk from the child to the public or section of the public.
- It would only be available if the child consented[436].
- It would most likely be offered shortly after the point of arrest and discovering of terrorism material in the child's possession.

7.89. The fundamental point is that if the destination of most criminal prosecutions is some form of non-custodial sentence comprising positive obligations, it is better to reach that point sooner. If that can be done without the stigma of a terrorism conviction, so much the better.

Modern Slavery

Generally

7.90. The codification of modern slavery is intended as a sword and a shield. As a sword, legislation that prohibits slavery and trafficking[437] is intended to aid detection of crimes that are often hidden, to punish and to deter. As a shield, the law is intended to be more accommodating to the special position of victims than previously has been the case.

[435] Defined by reference to sections 1, 2 Terrorism Act 2006, or section 58 Terrorism Act 2000.
[436] With legal advice, and in the presence of an appropriate adult.
[437] In this chapter I refer exclusively to the human trafficking aspect, rather than the "slavery" (slavery, servitude, forced or compulsory labour) aspect, of "modern slavery". Outside so-called Islamic State, I have not been made aware of any examples of terrorist "slavery", but there is an example of online influence being used to commit the offence of forced compulsory labour in the case of Matthew Felder ([2018] EWCA Crim 2514, a prolific and exceptionally sadistic sex offender). Felder was based in the UK but his victim was a 19-20 year old man in the United States [para 25].

7.91. In the terrorism prosecutions context, online recruitment has brought modern slavery (specifically, human trafficking) to the fore[438]. Online exploitation may be the flip side of online radicalisation, especially for children. CT Police and the Crown Prosecution Service have both noticed that allegations of modern slavery victimhood are now a feature of the landscape in youth prosecutions[439].

7.92. As the internet pulls more and more young people into criminal liability for terrorist offending, it is right that the authorities' approach to investigation and prosecution is reappraised, as there may be powerful personal or public interest reasons why a child or young person should not be prosecuted.

7.93. However, as discussed in this section, the application of modern slavery legislation and uncertain notions of victimhood risks poor outcomes in terrorism cases. An unwieldly counter-trafficking machinery complicates decision-making; inserts gross delays; and places too much decision-making power in the hands of modern slavery specialists who are likely to lack relevant information in the terrorist context.

7.94. Human nature is complicated, and individuals may be both subject to violence and coercion and genuine supporters of terrorism[440]. It is obvious that circumstances may mitigate, and exceptionally extinguish, culpability for terrorist acts, that children forced by proscribed organisations into soldiery are no less victims of terrorism[441], and that a child may be persuaded, bullied or blackmailed over the internet by members of a proscribed organisation or supporters of terrorism into joining them or committing a terrorist offence. Whether or not these exogenous circumstances are describable as modern slavery, the approach to assessing culpability and terrorist risk ought to be constant.

[438] Modern slavery is prominent in the context of travel to Syria (see for example, Report of the Inquiry by the All-Party Parliamentary Group on Trafficked Britons in Syria (2022)) although it has not, so far as I am aware, figured in any prosecution of a returning IS-supporter.
[439] There is one reported instance of a prosecution being dropped on modern slavery grounds: 'Terror case dropped against trafficking victim, aged 16' (BBC News, 27.1.22).
[440] As in the SIAC case of U3 v Secretary of State for the Home Department, SC/153/2018 & SC/153/2021 (4.3.22).
[441] UN Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism, 'UN expert affirms the rights of child victims of terrorism, urges human rights-based approach' (23.8.22).

7.95. However, in both the offline and online domains, distinctions between culpability and victimhood are not easily made, especially as circumstances stray from the core types of behaviour first prohibited by international law. As set out in the Palermo Protocol (2000)[442], trafficking is aimed at exploiting other human beings, where exploitation is defined in recognisable terms such as prostitution, forced labour, slavery or the removal of organs[443].

7.96. Agreeing under pressure, or being bullied into joining, a terrorist organisation as a result of online interactions, or agreeing to post terrorist manifestos or videos, is some distance from this type of core behaviour[444].

7.97. In its 2021 report, the Organisation for Security and Co-operation in Europe[445] makes strong points about the susceptibility of children to coercion, deception, and family pressure, and the use of human trafficking as a strategy by some terrorist groups including dedicated operations to entrap girls from deprived backgrounds as brides or suicide bombers. The internet plays a central role[446].

7.98. The report also notes areas of difficulty including the application of the non-punishment principle where individuals are subject to what the report refers to as "subtle means of trafficking" to commit grave crimes, such as terrorism[447]. Internet recruitment, where the individual is not in physical proximity to their recruiter, appears to fall within this category.

International Agreements

7.99. **Article 4** of the European Convention on Human Rights (1950) provides that no one should be held in slavery or servitude or required to perform forced or compulsory labour. Although no reference is made to trafficking in Article 4, decisions of the European Court of Human Rights have brought trafficking within its scope, but

[442] Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, adopted by the UN on 15.11.00 and ratified by the United Kingdom on 9.2.06.
[443] Article 3(a).
[444] Children forced into armed conflict are the subject of the Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict, adopted by the UN on 25.5.00.
[445] 'Trafficking in Human Beings and Terrorism' (2021).
[446] Ibid at p54.
[447] Ibid at p57. As examples of "subtle means" the report refers to confiscation of travel documents (p38) or abuse of power or a position of vulnerability (pp13, 19, 25, 41).

only where the elements of the Palermo Protocol and ECAT (see below) are satisfied[448].

7.100. The **Palermo Protocol** (2000) made specific provision for trafficking and was ratified by the United Kingdom in 2006[449]. The Protocol supplemented the UN Convention against Transnational Organised Crime and its focus was cross-border activity[450].

- It defined trafficking in persons as being for the purpose of "exploitation", with certain types of exploitation being identified "at a minimum", namely "…the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs"[451].
- States were required to prohibit such trafficking (at least), to protect its victims, and cooperate for its suppression[452].

7.101. The Council of European Convention on Action against Trafficking in Human Beings (2005) (also known as '**ECAT'**) came into force in the UK in 2009. It applied to both national and transnational trafficking, whether or not connected with organised crime[453].

- It defined exploitation in the same way as the Palermo Protocol and committed states to adopting measures to assist victims of trafficking, including a recovery and reflection period of at least 30 days "when there are reasonable grounds to believe that the person concerned is a victim"[454].
- Article 26 of ECAT contains a non-punishment provision which reads, "Each Party shall, in accordance with the basic principles of its legal system, provide

[448] See European Court of Human Rights, 'Guide on Article 4 of the European Convention on Human Rights' (last updated 31.8.22).
[449] Article 35 of the UN Convention on the Rights of the Child (1989), ratified by the UK in 1991, required states to take appropriate measures to prevent "the abduction of, the sale of or traffic in children for any purpose or in any form"; and Article 3 of the Option Protocol, ratified in 2009, required states to prohibit the offering, delivering or accepting of a child for the purpose of engagement of the child in forced labour. There are further measures regarding forms of Child Labour (e.g. the Worst Forms of Child Labour Convention, 1999, ratified by the UK in 2000).
[450] See Article 4.
[451] Article 3(2).
[452] Articles 5, 6, 9.
[453] Article 2.
[454] Article 12, 13.

for the possibility of not imposing penalties on victims for their involvement in unlawful activities, to the extent that they have been compelled to do so."

7.102. In 2011, the European Union adopted **EU Directive 2011/36** on preventing and combatting trafficking in human beings, which had effect from 6 April 2013[455].

- It required Member States to take necessary measures to penalise certain acts and provide assistance and support for victims.
- So far as the definition of trafficking was concerned, the minimum forms of exploitation contained in the Palermo Protocol and ECAT were extended to include "the exploitation of criminal activities"[456], with reference to the 1930 ILO Convention No 29 on Forced or Compulsory Labour[457].
- It contained a non-prosecution and non-punishment provision that required that Member States should, in accordance with the basic principles of their legal systems, take the necessary measures to ensure that competent national authorities are entitled not to prosecute or impose penalties on trafficking victims "for their involvement in criminal activities which they have been compelled to commit as a direct consequence" of trafficking[458].
- Like ECAT, the non-prosecution or non-punishment provision contemplated national authorities having considerable flexibility in whether and how to relieve individuals from criminal consequences where they had been "compelled" to commit offences through being trafficked.

7.103. The UK, then an EU Member State, opted into Directive 2011/36.

Identifying victims in the UK

7.104. In response to its ECAT obligations, the UK created the National Referral Mechanism, made up of Competent Authorities charged with making decisions on whether someone has been trafficked for the purposes of exploitation[459]. There is now a Single Competent Authority, which is part of the Home Office[460], and the Immigration

[455] The Palermo Protocol was previously supported in the EU by Framework Decision 2002/629/JHA.
[456] Article 2.3.
[457] Recital (11).
[458] Article 8.
[459] Cf Article 10. Following the implementation of the Modern Slavery Act 2015, the NRM was extended to all victims of modern slavery.
[460] See, Guidance, 'National referral mechanism guidance: adult (England and Wales)' (updated 19.5.22).

Enforcement Competent Authority which considers a specific set of adult cases in the immigration context[461].

- The Home Office has issued frequently updated statutory guidance for the identification of victims. The most recent version was issued in January 2023[462], and reflects the coming into force of the Slavery and Human Trafficking (Definition of Victim) Regulations 2022/ 877 which requires an element of travel before an individual can be identified as a trafficking victim.
- In defining whether a person is a victim of human trafficking, it states that a person must have been trafficked for the purpose of one or more of sexual exploitation; forced labour or services; slavery or practices similar to slavery; servitude; forced criminality; removal of organs[463].
- It follows that the guidance includes "forced criminality".
    - It will be recalled that "forced criminality" is not the subject matter of the Palermo Protocol or ECAT but was brought into scope by the EU Directive 2011/36.
    - Illustrations of "forced criminality" include activities like forced begging where an individual has been forced into criminal behaviour for another's financial gain[464].
    - Owing to the non-exhaustive nature of forced criminality, exploitation for terrorism purposes is potentially within scope.
    - However, the guidance refers back to the EU Directive (albeit the UK is no longer bound by it) and to the 1930 ILO Convention (No.29) concerning Forced or Compulsory Labour. It observes that the exploitation of a person for criminal activity "only falls within the scope of the definition of trafficking in human beings when all the elements of forced labour or services [under the ILO Convention] occur"[465].

7.105. The determination by the Single Competent Authority has two stages: a reasonable grounds stage, and then a conclusive grounds stage. The European Court of Human Rights has held that if the authority finds conclusively that a defendant is a

[461] These are foreign national offenders (FNO) cases where deportation is being actively pursued, non-FNO cases where removal is planned imminently or where an individual has been served a notice of intent informing them that their asylum claim is potentially inadmissible.
[462] Version 2.13. This is statutory guidance in England and Wales (under s49 Modern Slavery Act 2015) and non-statutory in Scotland and Northern Ireland.
[463] Para 2.22.
[464] Para 2.41.
[465] Para 2.44.

victim, then the CPS must have its own clear reasons if it disagrees with this assessment in any subsequent prosecution[466].

Modern Slavery Act 2015

7.106. In 2014, the UK adopted its own Modern Slavery Strategy[467]. The Modern Slavery Act 2015 is the principal domestic legislation governing the detection and eradication of modern slavery. The Act is predominantly concerned with penalisation and enforcement[468].

Definition of trafficking

7.107. Trafficking under the 2015 Act is based on arranging or facilitating another person's travel for the purposes of exploitation[469]. Caselaw suggests that the travel element may be minimal, but must still be present[470], although there are plausible arguments that the Palermo Protocol and ECAT do not require it [471]. An independent review of the 2015 Act in 2019 found that the Crown Prosecution Service took the view that trafficking included movement "over a very small space"[472].

7.108. However, in other respects the Act's definition of trafficking is much wider than the baseline minimum of core exploitation activities that the Palermo Protocol and ECAT, or the EU Directive, contemplate.

7.109. Alongside slavery, servitude, forced labour, sexual exploitation and the removal of organs, exploitation under the 2015 Act includes: (by section 3(5)) being subjected to force, threats or deception designed to induce him or her to provide services of any kind, provide another person with benefits of any kind, or enable another person to acquire benefits of any kind; and (by section 3(6)), using or attempting to use a child or vulnerable person for one of these purposes, having chosen them as a child or

[466] VCL and AN v United Kingdom, App.Nos. 77587/12 and 74603/12 (5 July 2021).
[467] November 2014.
[468] Parts 1-3.
[469] Section 2.
[470] Karameira [2018] EWCA 1432 at para 47; Ali [2015] EWCA Crim 1279 at paras 77-80. Both these cases relate to predecessor legislation.
[471] Anti-Slavery Commissioner, Annual report (2021-22) at para 2.3.11.
[472] Independent Review of the Modern Slavery Act 2015, 4th Interim Report (2019), at para 2.3.5.

vulnerable person, where a non-disabled adult would be likely to refuse to be used for these purposes.

7.110. This is apt to include forced criminality but goes much wider. There is no statutory requirement that any activity of this nature can only qualify if it would fall within the scope of the ILO Convention (No.29) on Forced or Compulsory Labour.

7.111. It is easy to see how online terrorist interactions can start to fall within the ambit of this broad definition. Subject to the minimal requirement of movement, the exploitation may take place online: threats or deception may be perpetrated online; "designed to induce" is a broad phrase; and the services or benefits which a person is induced to perform need not be criminal and may be minor. It is difficult to exclude recruiting a child to spray-paint a wall with a neo-Nazi slogan as being obviously outside the scope of services or benefits.

Section 45 defence

7.112. Part 5 of the 2015 Act is concerned with victims. For present purposes the most relevant provision is section 45, which establishes a modern slavery defence to criminal liability.

7.113. The first point to note is that a standalone defence is not mandated by any of the international agreements referred to above[473]. Prior to the 2015 Act, the UK's compliance with the non-prosecution and/or not-punishment provision was achieved by consideration of the public interest aspect of the Code for Crown Prosecutors, and subject to review by the courts under principles of abuse of process[474], as well as consideration of whether there was clear evidence of duress.

7.114. The purpose of section 45 was, according to Explanatory Notes accompanying the Bill[475], to make it more likely that victims would come forward to give evidence against their enslavers or traffickers without fear of being prosecuted themselves for any crimes for which they were responsible. The reality is that section 45 has simply established itself as a further defence to criminal liability of which defendants are naturally keen to take advantage.

[473] VCL and AN, supra, at para 158.
[474] See R v AGM [2022] EWCA Crim 920.
[475] At para 218.

7.115. The terms of section 45 are again wide, and piggy-back on the broad definition of exploitation in section 3. For adults it is a defence to do an act where he is compelled and the compulsion is attributable to slavery, or to exploitation within section 3 which is in turn attributable to human trafficking[476]. For children no compulsion is needed: it is sufficient that the act is done as a direct consequence of the child being or having been a victim of slavery, or of exploitation within section 3 which is attributable to human trafficking[477].

7.116. For children section 45 is doubly-innovative: no defence is required (see above), and absence of a requirement for compulsion goes beyond the requirements of the mandated non-prosecution or non-punishment provisions in ECAT and the EU Directive.

7.117. In each case the jury must ask whether a reasonable person in the defendant's position would have no alternative (adults) or would do (children) the act[478]. Once the defendant has adduced sufficient evidence to raise the defence as an issue, then prosecution must disprove it beyond reasonable doubt.

7.118. Section 45 therefore takes the requirement for non-prosecution or non-punishment provisions (ECAT, EU Directive) into generous territory:

- It provides a statutory defence to criminal liability, even in cases where the CPS consider that the public interest would otherwise warrant a prosecution.
- The defence dispenses with any requirement for compulsion in the case of children.
- It applies to victims of trafficking, where exploitation is widely defined, as well as slavery.

7.119. The application of section 45 defence is somewhat mitigated by the exclusion of certain offences, listed in Schedule 4 of the Act and amendable by statutory

[476] Section 45(1)-(3). Because the section 45 defence depends in part on being attributable to human trafficking, it is possible to spot a potential divergence between victimhood under section 45 and victimhood as considered by the Single Competent Authority using the statutory guidance. Where "human trafficking" means human trafficking as defined by section 2, then some element of travel is required. Where "human trafficking" means human trafficking as defined by the guidance, then no travel element is needed.
[477] Section 45(4).
[478] Section 45(1)(d) and 4(c).

instrument. The included offences were described in the Explanatory Notes to the Bill as 'certain serious offences'[479].

7.120. The scheduled offences are a mixture of obviously grave common law or statutory offences such as murder, kidnapping, robbery, possession of firearms with intent, violence and a wide range of sexual offences. Judging by their maximum sentence, some of these offences are in the more moderate category: for example, section 20 (malicious wounding, 5 years) section 16 (threat to kill, 10 years) section 37 (assaulting an officer preserving a wreck, 7 years) Offences Against the Person Act 1861.

7.121. In the field of national security, Schedule 4 includes offences relating to hostages, aviation, explosives, nuclear weapons and a limited number of offences under terrorism legislation. These are:

- Sections 54 (weapons training), 56 (directing terrorism organisation), 57 (possession of article for terrorist purposes) and 59 (inciting terrorism overseas) under the Terrorism Act 2000.
- Sections 5 (attack planning), 6 (training), and 9-11 (radioactive devices).

7.122. It will be seen that many commonly encountered terrorism offences are excluded such as section 58 (collection of information useful to terrorists) Terrorism Act 2000 and sections 1 (encouragement) and 2 (terrorist publications) Terrorism Act 2006.

Analysis

7.123. As casework is demonstrating, the statutory modern slavery defence is capable of being relevant to terrorism prosecutions.

7.124. The definition of exploitation is broad and could encompass exploitation of an individual by a terrorist group or individual terrorist who is encountered solely online. It is not difficult for a defendant, especially if he is a child, to raise an issue under the section 45 defence.

[479] Para 218.

- It is true that a person could not be treated as a victim of trafficking under the 2015 Act or identified as a victim of trafficking under the Slavery and Human Trafficking (Definition of Victim) Regulations 2022 if they stayed in front of their computer screen at all times;
- However, if their online recruitment raised some element of movement, however minimal – if, for example, they were recruited to go into town to sit outside the local police station and note the number plates of police officers and staff (which could be used for future targeting purposes[480]) – then human trafficking could arise.

7.125. It follows that the possible existence of a section 45 defence is something that will often need to be considered during investigations; when considering the sufficiency of evidence; during any trial; in addition to considering the possible victim status of the defendant in connection with the overall public interest in prosecution.

7.126. The complexity of the assessment of victimhood results from the fact that – in criminal terrorism cases – there are two separate categories of assessor.

- On the one hand, the Single Competent Authority determines victimhood applying the statutory guidance, and a 2-stage process (reasonable grounds/ conclusive grounds). The SCA may or may not (and if there is sensitive information is unlikely to) know the full picture of whether the defendant was a radicaliser himself, or a victim of others.
- On the criminal justice side, the polic and CPS need to consider victimhood in relation to the section 45 defence, under their evidential assessment, and also as part of the public interest assessment in whether to prosecute.

7.127. Since the CPS's guidance on modern slavery[481] requires that in principle decisions to prosecute should be delayed whilst the Single Competent Authority is conducting its assessment, this raises acute issues of delay with practical consequences in terrorism cases:

[480] Contrary to section 58 Terrorism Act 2000.
[481] *Supra*, under 'The Single Competent Authority decisions and the decision to prosecute' and 'Decisions to prosecute whilst awaiting an SCA decision'.

- I am informed that even in youth terrorism cases, the Single Competent Authority has in one instance required 7 months to reach a conclusive grounds decision.
- There are instances of suspects or defendants seeking to challenge negative decisions by the SCA, adding further delay.
- If a child has not been charged, they will be left in limbo and potentially subject to stringent bail conditions for a long period of time.
- If a child has been charged and remanded in custody because of their exceptional risk, delay will extend pre-trial custody and could require their release on bail.
- Even if after all this time the SCA determines against victimhood, the criminal justice agencies will still need to consider the section 45 defence.

7.128. The primacy of the Single Competent Authority in assessing victimhood is now a feature of the landscape[482]. The involvement of this separate agency adds huge uncertainty about how terrorism prosecutions may play out, and what that means for risk management.

7.129. Steps will no doubt be taken – and are required to be taken – to ensure that the SCA's decision-making is sped up. It is of course proper and inevitable that SCA will on occasion reach conclusions that CT Police disagree with or find inconvenient: but not if the SCA's decision-making is qualified by lack of access to relevant information.

7.130. One modest step could however be taken to reduce the complexity in terrorism cases, and that is to extend Schedule 4 Modern Slavey Act 2015 to encompass all terrorism offences. The result would be that the section 45 defence would not be available for terrorism offences. As explained already, a special statutory defence, let alone a statutory defence of the width created by section 45, is not a requirement of any of the agreements to which the UK is (or in the case of the EU Directive, has been) party.

7.131. Amending Schedule 4 in this way would reflect that:

[482] See VCL, supra.

(a) All terrorism offences are serious. Even pre-cursor terrorism offences now carry significant maximum penalties[483].

(b) The purpose of all terrorism offences is to forestall terrorist violence. Since violent offences are included within Schedule 4 it would be consistent to include terrorism offences that aim at preventing yet more serious violence. A subject-matter approach is not objectionable (cf the inclusion of most sexual offences).

(c) Terrorism prosecutions are investigated and prosecuted by specialist police and prosecutors. The Counter Terrorism Division of the Crown Prosecution Service gives minute attention to the public interest in prosecution including whether the defendant is in some senses a victim. A separate modern slavery defence is not needed to ensure that victims are not made criminally liable.

(d) The option of relying on repeat offending (despite warnings or cautions) as a means of demonstrating voluntariness and seeking to negative the section 45 defence in relation to the later offence[484] is not palatable in the context of terrorism.

7.132. A further complexity - which this option would remove – comes from the fact that a variety of terrorism offences is often prosecuted in a single case: for example, attack-planning together with possession of useful information; or possession of an article with terrorist intent together with encouragement. In both these examples, one offence is already within Schedule 4 and exempt from the section 45 defence, the other is not. For the avoidance of doubt, none of this would remove the obligation of police and prosecutors to consider the possibility of trafficking when assessing the public interest in whether to prosecute.

7.133. I therefore **recommend** that Schedule 4 Modern Slavery Act 2015 is amended to include all terrorism offences.

Sentencing

[483] Section 58 Terrorism Act 2000 (up from 10) and sections 1 and 2 Terrorism Act 2006 (up from 7) all carry a maximum of 15 years following amendment by the Counter-Terrorism and Border Security Act 2019.
[484] I have been informed that prosecutors take this approach with other types of offending: for example, where an individual has been acquitted of drugs trafficking on the basis of section 45, a prosecutor may argue that further drugs offending (on the particular facts) must be voluntary and unaffected by trafficking.

7.134. The most common type of sentence imposed on conviction for a terrorism offence in 2021 was a sentence of between 1 and 4 years' imprisonment (16). Next were sentences of between 4 and 10 years' imprisonment (12), and after that, 11 instances of non-custodial sentences and 7 sentences of under one year[485].

7.135. Child sentences are most likely to fall within the non-custodial bracket, whilst the lower end custodial sentences are likely to include failures to comply with TPIMs and post-release measures. There were 2 life sentences.

7.136. At the end of 2021, the prisons held (including on remand) 154 Islamist terrorist prisoners, 52 Extreme Right Wing terrorist prisoners, and 23 other terrorist prisoners[486]. The vast majority (187 out of 229) were British[487]; 79 were White people as against 150 who described themselves as having mixed, Asian, Black or other ethnicity[488]. There were slightly more self-declared Muslim terrorism-connected prisoners (159) than had been convicted for Islamist terrorism offences (154)[489].

SCPO

7.137. Serious Crime Prevention Orders are now frequently imposed following conviction, to ensure an even greater degree of control over than licence conditions or post-release obligations[490]. Daniel Hannam, the neo-Nazi former police probationer, must comply with measures relating to his use of the internet to protect the public after his release[491].

7.138. There were 15 SCPOs obtained in terrorism-related cases in 2021. The Home Office is currently doing a review of SCPOs generally.

Part 4 CTA 2008

7.139. After Usman Khan's attack at Fishmongers' Hall in London in 2019, there is greater and more coordinated monitoring of released terrorist offenders. This is

[485] Table A-C.04.
[486] Table A-P.01.
[487] Table A-P.03.
[488] Table A-P.02.
[489] Table A-P.04.
[490] Under Part 4 Counter-Terrorism Act 2008.
[491] CPS, 'Former police officer jailed for National Action membership' (News, 30.4.21).

reflected in the number of cases (6) brought by the CPS under the Counter-Terrorism Act 2008, which contains the notification obligations applicable after release[492].

7.140. During 2021:

- the Court of Appeal considered the application of these provisions to work vehicles – they applied, despite the inconvenience[493].
- Ismail Abdurahman, who had assisted one of the 21/7 failed suicide bombers, was sentenced to 8 months' imprisonment for failing to notify the police of his new phone number, email and vehicle[494].

[492] Table A-C.02.
[493] R v R [2021] EWCA Crim 35.
[494] 'Man convicted for terrorism offences back in jail for breaching release conditions' (Southwark News, 6.8.21).

8. SPECIAL CIVIL POWERS

8.1. Counter-terrorism has always dealt in disruption and risk management, and the list of methods has steadily grown. Some of these are immigration and nationality-related powers harnessed to counter-terrorism ends such as deportation, exclusion, refusal of naturalisation and deprivation of citizenship.

8.2. These powers, which may apply to suspected spies as much as to suspected terrorists, fall outside the scope of the Independent Reviewer of Terrorism Legislation. In 2021 the powers were exercised as follows[495]:

- Removal of passport facilities: once for national security reasons.
- Exclusion from the United Kingdom: 14 times for national security reasons.
- Deprivation of citizenship: 8 times on the basis that it was 'conducive to the public good' (which includes, but is not limited to, national security reasons).

8.3. Other special terrorism powers do fall within the Reviewer's remit and are considered in this Chapter.

8.4. Firstly, Terrorism Prevention and Investigation Measures ('TPIMs') offer a strong power of disruption, falling short of imprisonment, based on sources of evidence that could not be used in criminal proceedings. They are the direct successors to Control Orders, which were created by the Prevention of Terrorism Act 2005. This Chapter contains my discretionary annual review of the operation of the Terrorism Prevention and Investigations Measures Act 2011 for the calendar year 2021[496].

8.5. Secondly, Serious Crime Prevention Orders, grantable by the High Court even the absence of any conviction.

8.6. Thirdly, Temporary Exclusion Orders ('TEOs') which were created by the Counter-Terrorism and Security Act 2015 principally to manage the risk posed by the return of British citizens from territories controlled by Islamic State.

[495] HM Government, Transparency Report (2022).
[496] For the calendar year 2022 I will have a statutory obligation to report annually: section 41 Counter-Terrorism and Sentencing Act 2021.

8.7. Fourthly, the power to seize passports under Schedule 1 to the Counter-Terrorism and Security Act 2015, to enable the authorities to determine whether to invoke one of the powers above.

8.8. Finally, financial freezing measures under the Anti-Terrorism Crime and Security Act 2015.

TPIMS

8.9. The preventive measures provided for by the Terrorism Prevention and Investigations Act 2011 include, at their sharpest, a requirement to live in Home Office provided premises in a different part of the country and have been used, less dramatically but showing the degree to which TPIMs intrude on day-to-day freedomsto prohibit the possession of non-approved kitchen knives.

8.10. A typical feature of TPIMs is a package of restrictions on electronic communications. Being limited to using a fixed landline was manageable at the time of the Prevention of Terrorism Act 2005. But constant access to a smartphone is now essential for some gig-economy type work. Given that paid work is often a stabilising factor with significant benefit in terms of managing national security risk, the onus is officials to find ways of accommodating modern work with communications measures. I am aware of one case where a desire to work (supported by officials) clashed with rigid restrictions on communications.

8.11. The regime has undergone various amendments since 2011. Parliament re-authorised the regime for a further 5-year period in November 2021[497]. It remains justified for a small number of cases that cannot be managed in any other way.

8.12. In June 2021, further significant changes came into force with Counter-Terrorism and Sentencing Act 2021.

8.13. The most important of these was the power to maintain a TPIM for up to 5 years[498]. This change will apply to fresh TPIMs made after June 2021[499].

[497] Terrorism Prevention and Investigation Measures Act 2011 (Continuation) Order 2021.
[498] Section 35 of the 2021 Act.
[499] No TPIMs were in fact made during the second part of 2021.

8.14. Further changes made by the 2021 Act were:

- Lowering the threshold for the Secretary of State's assessment of past involvement in terrorism-related activity from 'satisfied on the balance of probabilities' to 'reasonably believes'. Although the phrase 'reasonable belief' may be more apposite when dealing with the evaluation of intelligence, it remains to be seen what if any practical effect this has, particularly in the context of section 9 review hearings.
- Adding an express power for the Secretary of State to vary a residence measure on the basis of resources. The High Court will, on any review of the use of this power, will have to descend into the arena of resources – something that it has traditionally been unwilling to do[500]. This power was not used in 2021.
- Enabling the residence measure to require individuals to remain at home not only during an overnight period, subject to the overriding restrictions of Article 5 ECHR. This power was not used in 2021.
- Enabling the use of polygraphs on TPIM subjects. This power was not used in 2021 but the relevant regulations are now in force (from 2022)[501].
- Providing for the possibility of drugs-testing measures. This power was not used in 2021, but it is consistent with the changing TPIM cohort – not so much hardened ideologues as chaotic (but still potentially dangerous) individuals.
- Adding further information requirements, intended to exclude uncertainty about where a TPIM subject is living (assuming they have not been relocated), and the electronic devices which are within the TPIM subject's household. Three existing TPIMs were changed during 2021 to require the provision of information about electronic devices.

TPIMs in 2021

8.15. In preparation for this report I have attended the quarterly TPIM Review Group ('TRG') meetings chaired by Home Official officials on current TPIMs, or read and discussed the minutes where I have been unable to attend, discussed individual cases and thematic issues with officials, followed the progress of current TPIM cases, and

[500] QX v Secretary of State for the Home Department [2022] EWHC 836. para 66, in the context of TEOs.
[501] The Terrorism Prevention and Investigation Measures (Polygraph) Regulations 2022.

considered the open and closed papers lodged by the Home Office, and documents and legal pleadings provided by TPIM subjects.

8.16. As to whether a TPIM can be modified or revoked, MI5 hold the whip hand, because it is their operational assessment of risk that is likely to be determinative of the advice passed to the Home Secretary. However, there continues to be a strong degree of challenge by the Home Office TRG-chair. The overall TRG process has improved with separate consideration of each measure, providing an opportunity for a liberalising tweak. The degree of consideration for each TPIM measure was impressive.

8.17. During 2021, as has been the case throughout the history of the legislation, no TPIM came to an end other than by expiry by reason of time, or revocation.

8.18. In last year's annual report, I drew attention to the 'TPIM Catch-22'[502], my phrase to describe the risk that TPIM subjects, whether they appeared to be compliant or not, might find it impossible to demonstrate reduction in their risk to the satisfaction of MI5. I recommended that the Home Office should seek to formulate guidance on evaluating risk reduction, so that TPIMs did not become impossible to remove.

8.19. I welcome the government's partial acceptance of this recommendation. Home Office officials will now support MI5 to establish whether guiding principles can be developed for use in relation to TPIM cases to enhance the review process, and improve assurance that as time passes each TPIM continues to be necessary and proportionate. This should ensure that past learning is retained; consistency is improved; and the Secretary of State, when she is asked to maintain or extend a TPIM, should have greater reassurance that reductions or testing opportunities have been considered. I have seen already seen evidence of a more proactive approach to testing opportunities, which is to be welcomed.

8.20. The government publishes quarterly information in the form of written ministerial statements about the use of TPIMs. The 5 ministerial statements covering 2021 reveal the following:

[502] Terrorism Acts in 2020 at 8.22 et seq.

- During the quarter ending Feb 2021[503], there were 3 TPIMs in force (2 relocations) including one extension of an existing TPIM.
- During the quarter ending May 2021[504], 5 TPIMs were in force (4 relocations), of which 3 were new including 2 relating to alleged attack-planners[505]. One had expired.
- During the quarter ending August 2021[506], 5 TPIMs were in force (3 relocations), of which 1 was new. One was revoked.
- During the quarter ending November 2021[507], 4 TPIMs were in force (2 relocations), after one (JM) had expired.
- During the quarter ending February 2022[508], 2 TPIMs were in force (1 relocation), after one was revoked and one had expired (HB).

8.21. All TPIM subjects during 2021 were British citizens. As with all previous TPIMs (and control orders) all TPIM subjects in 2021 were assessed to be Islamist terrorists.

8.22. From my observations and conversations with officials, it is also clear that mental health and neurodivergence are now firmly on the TPIM agenda and there is greater use of psychological support to understand behaviour and improve communication. The existence of drugs testing measures are indicative of a new, less stable, cohort; the Home Office and Security Service will have to learn to assess and manage individuals who may, for example, require medication as part of their day to day living. TPIMs should not be allowed to cross into areas of compulsory medical treatment that are regulated by different legislation[509].

8.23. During 2021 the first sustained challenge was made to the intervention process. The immediate point of contention was the undermining of legal professional privilege. Unlike the hardened Al-Muhajiroun ideologues, it is possible to observe in the new set of TPIM subjects the prospect of more positive outcomes from mandated meetings with intervention providers (whether ideological or practical): people with neurodivergence or poor mental health may welcome and come to rely on

[503] HCWS926 (20.4.21).
[504] HCWS161 (8.7.21).
[505] TL is also said to have autism: SSHD v TL [2022] EWHC 825 (Admin) at para 2.
[506] HCWS343 (21.10.21).
[507] HCWS632 (24.2.22).
[508] HCWS105 (16.6.22).
[509] Principally, the Mental Health Act 1983.

professional structured intervention. These individuals may already be isolated; indeed the effect of TPIMs can lead to further isolation.

8.24. The government accepted my recommendation that psychologists should be more involved in the TRG process, and again I have seen evidence of this in action[510].

8.25. There was one significant judgment during 2021, which concerned a review of TPIMs imposed in 2019 against two members of Al-Muhajiroun[511]. I considered this judgment fully in last year's annual report.

Breaches in 2021

8.26. TPIM breaches are criminal offences, and suspected breaches leading to charges, remands into custody, and revocation of the TPIM (subject to revival on release[512]) are now a constant feature of the TPIM landscape. By the end of 2021, only 2 TPIMs were in force; 4 TPIMs would have been in force but had been revoked because of breaches or alleged breaches.

- In February, LF was sentenced to 2 years 4 months.
- In June, QB was sentenced to an 18 months' community order[513].
- In October, one TPIM subject was charged with a breach.
- In December, a further TPIM subject was charged with 5 breaches of the communication measures.

8.27. Chaotic individuals may be more liable to breach the numerous and detailed requirements that TPIMs impose. I am aware that the CPS look carefully at the full circumstances when deciding whether the public interest calls for prosecution, but TPIM subjects should avoid being set up to fail. Otherwise a TPIM is not really a tool for managing risk in the community, but a speedy route to prison.

High Court SCPOs

[510] There is more already integration of psychologists in the prison, MAPPA and Prevent processes.
[511] Secretary of State for the Home Department v JM and LF [2021] EWHC 266 (Admin).
[512] Section 13(6).
[513] 'Member of banned group beached anti-terror order for sex, court hears', (BBC News, 2.6.21).

8.28. In 2021, 13 terrorism-related Serious Crime Prevention Orders ('SCPOs') were imposed in criminal proceedings in the Crown Court following application by the Crown Prosecution Service[514]. However, no terrorism-related SCPOs have been sought to date in the High Court, despite the recent widening of the class of applicants to include CT Police[515]. Indeed, standalone High Court orders remain something of a rarity[516].

1.1. As long as the civil route remains untested in terrorism-related cases, the authorities will continue to have fears regarding, above all, the disclosure process. SCPOs are not available for children.

TEOs

8.29. Temporary Exclusions Orders are hybrid orders. On the one hand they exclude British citizens from returning other than in accordance with a 'permit to return' which allows the authorities to determine how when and where they will return to the United Kingdom[517]. The High Court has held that this aspect of TEOs is a form of immigration control and that any challenge to this aspect therefore attracts a reduced measure of procedural protections[518].

8.30. On the other hand, TEOs permit the authorities to impose a selection of the measures available in TPIM cases which operate for a non-renewable period of up to 2 years on return: such measures are likely to interfere with a TEO subject's fundamental rights and freedoms and so, the High Court held, a more generous measure of procedural protection applies[519].

8.31. It is of course open to the Secretary of State to impose a TPIM, with greater control measures, on a person who has returned from overseas (for example, Syria). The fact that TEOs permit fewer control measures and may be imposed on the basis of reasonable suspicion of past involvement in terrorism-related activity[520], suggests

[514] HMG, Transparency Report (2022).
[515] Schedule 12 to Counter-Terrorism and Sentencing Act 2021.
[516] The only recent example I am aware of is the first and only Scottish case of David Collins, who had made numerous firearms threats: 'Man 'addicted' to firearms given Scotland's first standalone SCPO' (Crown Office and Procurator Fiscal Service, Media Release, 8.10.20).
[517] Section 5 Counter-Terrorism and Security Act 2015.
[518] QX v Secretary of State for the Home Department [2020] EWHC 1221, at para 56, Farbey J.
[519] Ibid, at para 68.
[520] Condition A, section 2(3) of the 2015 Act.

that they are designed to deal with individuals on a precautionary basis, rather than where there is specific intelligence that an individual poses a terrorist threat.

8.32. The Secretary of State's expectation has been that judicial review challenges to TEOs would be more summary affairs than statutory reviews of TPIMs. In practice, her expectation was that a Security Service witness would not be required to prepare a witness statement or attend for cross-examination. The High Court has recently decided that this approach is not always sufficient[521]; the government's appeal is outstanding.

8.33. In 2021, five (5) TEOs were imposed on four (4) males and one (1) female. Of the five TEOs imposed in 2021, four returned to the UK in 2021 (3 males, 1 female) and one returned in 2022 (male)[522].

8.34. TEOs are only available for individuals with the right of abode in the United Kingdom, and would therefore not have been available in the case of Shamima Begum had the Court of Appeal's decision, to allow her to return to the UK to contest her citizenship deprivation, been upheld by the Supreme Court[523].

Passport Seizure and Retention

8.35. The temporary[524] seizure of passports is intended to allow the authorities to investigate an individual whilst they remain in the country, and consider measures such as prosecution, passport removal, or TPIMs.

8.36. This power was used once in 2021[525], a level which reflects how far things have moved from the heyday of jihadi travel to Syria and Iraq in the previous decade, and the impact of COVID.

Money Measures

[521] QX v Secretary of State for the Home Department [2022] EWHC 836, at paras 85-6, Farbey J.
[522] Transparency Report 2022.
[523] R (on the application of Begum) v Secretary of State for the Home Department [2021] UKSC 7.
[524] 14 days extendable on court application to 30 days: Schedule 1 to Counter-Terrorism and Security Act 2015.
[525] Transparency Report 2021 (published 2022).

8.37. Special detention freezing and forfeiture powers are provided by the Anti-Terrorism Crime and Security Act 2001. These powers apply to property which consists of resources of a proscribed organisation or property that was obtained through or is intended for use in terrorism[526]. They are therefore wider than general forfeiture powers found under the Proceeds of Crime Act 2002 which depend upon identifying specific offences through which the property was obtained or for which it is intended, and do not apply to sums below a specified minimum amount (currently £1,000)[527]. In practice, CT Police make use of both regimes.

8.38. In May 2021 the Metropolitan Police applied for Account Freezing Orders against accounts in Northern Ireland under the 2001 Act. This was done in collaboration with the PSNI and in connection with Operation Arbacia, the major operation being conducted against the New IRA. These orders were voluntarily discharged – on the basis they should have been sought before the Belfast court – and further orders were granted later the same month. The Northern Ireland High Court upheld these orders even though it found that, contrary to the statutory requirement, PSNI had not consulted the Treasury before its applications in Northern Ireland[528].

8.39. Cross-border enforcement of Account Freezing Orders obtained within different parts of the United Kingdom is provided for by the Civil Judgments and Jurisdictions Act 1982[529]. There are procedural requirements, but although their complexity was drawn to my attention by CT Police, any difficulties seemed to be down to lack of familiarity as opposed to the mechanisms being intrinsically unsuitable to CT operations.

8.40. In next year's report I will consider amendments to the freezing and forfeiture regime under Schedule 1 to the Anti-Terrorism, Crime and Security Act 2001 which are currently before Parliament[530]. Assuming they are enacted, they will expand the freezing and forfeiture regime to cryptocurrency.

---

[526] Section 1 and Schedule 1.
[527] Part 5.
[528] In the matter of applications by Amanda Duffy and others [2021] NIQB 114. The purpose is to enable the Treasury to consider the alternative of designating a person under sanctions powers: para 68-9. the person Metropolitan Police had consulted the Treasury before the application to Westminster Magistrates' Court.
[529] Section 18(4ZB).
[530] Within the Economic Crime and Corporate Transparency Bill.

9. NORTHERN IRELAND

Introduction

9.1. Compared to the rest of the United Kingdom, terrorism and counter-terrorism have a different aspect in Northern Ireland, although the Terrorism Act 2000 had its origin in the temporary measures used in the 1970s against Northern-Ireland Related Terrorism ('NIRT'), and the Terrorism Acts apply equally to Northern Ireland. National security is an 'excepted matter' under the Northern Ireland Act 1998[531].

9.2. Some of the reasons for this different aspect are as follows:

- Firstly, because of the legacy of the Troubles. Northern Ireland was, and remains, affected with higher levels of violence and use of firearms and munitions arising from the activities of proscribed organisations (referred to in Northern Ireland as paramilitaries) than occur elsewhere in the UK. This was reflected in figures reported by the UK to Europol (pre-Brexit): in the last few years security incidents in the UK were dominated by incidents in Northern Ireland[532]. Conversely, the threat from Islamist terrorism in Nothern Ireland is much lower than elsewhere in the UK.
- Secondly, and relatedly, the targeting of police and the broader state apparatus has tended to require a greater degree of security adjustment than apparent elsewhere, such as routinely armed police, the common use of armoured vehicles, and special security for judges. The main findings of His Honour Brian Barker CBE KC's report in his capacity as the Independent Reviewer of National Security Arrangements in Northern Ireland dealing with the period from 1 January 2021 to 31 December 2021 were set out in a written statement from the Secretary of State for Northern Ireland in June 2022.[533]
- Thirdly, the special stop and search powers that exist in Northern Ireland under the Justice and Security (Northern Ireland) Act 2007, which have more impact on the population of Northern Ireland than Terrorism Act powers. Professor Marie Breen-Smyth, newly-appointed Independent Reviewer of the Justice

[531] I am particularly grateful to Karl Laird, one of my special advisers, for his work on this Chapter.
[532] In 2020, Northern Ireland accounted for 56 out of 62 UK terrorist incidents: Europol, TE-SAT Report 2021, page 12.
[533] Hansard (HC) Vol. 717 Col. 35WS.

and Security (Northern Ireland) Act 2007, published her first report covering the period 1 August 2020 to 31 July 2021 in June 2022.

- Fourthly, and related to the legacy of the Troubles[534], counter-terrorism policing is a more controversial activity than it is in Great Britain. There is accordingly greater reluctance on the part of police and politicians to refer to terrorist threats and counter-terrorism successes.

9.3. Online terrorism wears a different aspect too in Northern Ireland. It was suggested to me that online activity is not so much – as in Great Britain – a route into terrorist groups, know-how, and ideology. Physical paramilitary groups rooted in local areas can already provide this. If anything, online activity appears to be a distraction away from traditional paramilitary behaviour for many groups such as meetings, training, parading, and drug-dealing.

9.4. However, although in general proscribed organisations have not used the internet as a direct encouragement to violence, Dissident Republican groups such as the new IRA and Continuity IRA use online activity as a tool to seek community support and recruits, to undermine normalisation of policing, to generate sympathy and support for prisoners on remand awaiting trial for terrorism, and to push their particular narrative. This may be done by deploying wedge issues or preoccupations such as Israel/Palestine, the gilet jaune movement in France, local gold mines, or the Northern Ireland Protocol.

9.5. PSNI have an impressively run Digital Intelligence Hub, which performs some of the functions of CTIRU[535] in liaising with service providers on content moderation issues.

9.6. I am pleased to report that the Northern Ireland Office has now started publishing statistics relating to the Terrorism Act 2000, the Terrorism (Northern Ireland) Act 2006, the Counter-Terrorism Act 2008, and the Justice and Security (Northern Ireland) Act 2007 on a calendar year basis. This will facilitate comparisons with statistics from Great Britain.

The Northern Ireland Security Situation

[534] In July 2021, the government published a Command Paper, 'Addressing the Legacy of Northern Ireland's Past' (CP 498) which led to the introduction in 2022 of the Northern Ireland Troubles (Legacy and Reconciliation) Bill.
[535] See Chapter 1.

9.7. In 2021 the threat level in Northern Ireland from Northern Ireland-related terrorism remained at "*severe*" (meaning that an attack is highly likely), although it was to be reduced to an unprecedented level[536] of *"substantial"* in March 2022. The threat posed specifically by Northern Ireland-related terrorism to Great Britain, as opposed to other forms of terrorism, is no longer published separately.

9.8. The principal terrorist threat in Northern Ireland emanates from two groups – the new IRA (nIRA) and the Continuity IRA (CIRA). Other smaller groups, such as Arm na Poblachta (ANP) and Oglaigh na h/Eireann (ONH) may retain the intent to carry out attacks but are likely to lack the capability to do so.

9.9. So far as the calendar year 2021 was concerned:

- There were no "*national security attacks*".[537]
- Two civilians were killed as a result of "*deaths attributable to the security situation*".[538]
- There were 27 shooting incidents (12 less than the previous year) and 5 bombing incidents, in which 5 bombing devices were used in connection with the "*security situation*" (17 less than the previous year).[539]
- There was a total of 51 casualties as a result of "*paramilitary-style attacks*".[540]
- These paramilitary attacks were made up of 14 "*paramilitary style shootings*" (4 committed by Loyalist groups and 10 by Republican groups) and 37 "*paramilitary style assaults*" (33 committed by Loyalist groups and 4 by Republican groups).[541]
- The PSNI recovered 39 firearms, 1,002 rounds of ammunition, and 0kg of explosives.[542]

9.10. The weapons generally used by nIRA and CIRA include firearms or small improvised explosive devices (such as pipe bombs), but they have also deployed larger and potentially more destructive devices such as vehicle borne improvised

[536] For Northern Ireland.
[537] As deemed by the PSNI.
[538] PSNI, Security Situation Statistics, information up to and including March 2022, Table 3.
[539] Ibid, Table 5.
[540] Ibid, Table 4.
[541] Ibid, Table 4.
[542] Ibid, Table 6.

explosive devices and explosive projectiles. In 2021, pipe bombs were found during investigations into terrorism-related offences, and in other cases where a link to terrorism could not be confirmed.

9.11. In mid-March 2021, a shooting was directed at Enniskillen police station using a homemade firearm. No casualties were reported. It was believed that CIRA were responsible for this incident. In April 2021, an improvised explosive device was deployed targeting an off duty police officer in Dungiven, however the device failed to function. This attacked is believed to have been conducted by nIRA.[543]

9.12. PSNI's concerted action against nIRA, under the umbrella of Operation Arbacia, led to yet further arrests during 2021. By March 2021 8 men and 2 women had been charged. Criminal proceedings are ongoing.

Terrorist Groups in Northern Ireland

9.13. In 2021 there was no change to the list of 14 proscribed organisations in Northern Ireland, a list that has remained unaltered since before the enactment of the Terrorism Act 2000. I continue to be of the view that the failure to weed out defunct groups such as Cumann na mBan demonstrates that the proscription regime as it applies in Northern Ireland is wanting[544].

9.14. For the reasons I gave in last year's report, the devolution settlement calls into question how effectively decisions about proscription can be made by the Secretary of State for Northern Ireland.[545]

9.15. The issue is one of transparency between different public bodies, all of which ultimately have the same goal. Progress to ensure that the devolved institutions can engage directly with the Northern Ireland Office on matters which relate to national security is needed. The baleful influence of paramilitary groups on day to day life remains a feature of Northern Ireland.

Investigations

[543] Europol, TE-SAT Report 2022, pages 74-75.
[544] In December 2021, the Independent Reporting Commission, in its 4th Report (HC 916) referred to removal from the list of proscribed terrorist organisations in the context of group transition: para 4.12.
[545] Terrorism Acts in 2020 at 9.17-9.18.

9.16. In this part, I consider stop and search powers, and the use of police cordons, in Northern Ireland. Other terrorism powers which are available in Northern Ireland are considered in Chapter 4.

Stop, Search and Question

9.17. The powers of stop and search in sections 43, 43A, and 47A of the Terrorism Act 2000 exist alongside the more widely used powers in the Justice and Security (Northern Ireland) Act 2007. In summary, the most relevant powers in the 2007 Act are:

- Section 21 - A power to stop a person for so long as is necessary to question them to ascertain their identity and movements. There is also a power to stop a person for so long as is necessary to question them to ascertain: (a) what they know about a recent explosion or another recent incident endangering life; (b) what they know about a person killed or injured in a recent explosion or incident. It is an offence for a person to fail to stop; to fail to answer a question; or to fail to answer to the best of their knowledge and ability a question which has been addressed to them. This power includes a power to stop vehicles.

- Section 23 - A power to enter any premises if it is considered necessary in the course of operations for the preservation of peace or the maintenance of order. An authorisation from an officer of at least the rank of superintendent must be obtained before this power can be exercised, unless it is not reasonably practicable to obtain authorisation.

- Section 24/Schedule 3, paragraph 2 - A power to enter any premises for the purpose of ascertaining whether there are any munitions unlawfully on the premises, or whether there is any wireless apparatus on the premises. An officer may not enter a dwelling unless he is an authorised officer and they reasonably suspect that the dwelling unlawfully contains munitions or contains wireless apparatus.

- Section 24/Schedule 3, paragraph 4 - A power to stop and search a person whom a constable reasonably suspects to have munitions unlawfully on them or to have wireless apparatus on them.

- Section 26/Schedule 3 - These provisions extend the power to search premises to stop vehicles and to take a vehicle to any place for the purposes of carrying out a search. It is an offence to fail to stop a vehicle.

9.18. In her annual report Professor Marie Breen-Smyth points out that there is an overall downward trend in the use of stop and search under all powers in Northern Ireland from the highest levels from 2008, alongside a fairly consistent use of PACE powers.[546] She draws attention to a decrease in the number of stop and searches under section 24 (down by 14%) and section 21 (down by 31%). Professor Breen-Smyth observes that should this downward trend in the use of the powers in the Justice and Security (Northern Ireland) Act 2007 continue, it will mark a transition of policing from the use of exceptional powers towards harmonisation with practice elsewhere in the United Kingdom. This is a welcome trend which will hopefully continue in the years to come[547].

9.19. As far as the powers in the Terrorism Act 2000 are concerned, the table below shows how frequently the stop and search powers in section 43, 43A and 47A of the Terrorism Act 2000 have been used in Northern Ireland since 2014, by calendar year.[548] It also shows the frequency with which the comparable powers in the Justice and Security (Northern Ireland) Act 2007 have been used. The reference to "*TACT in conjunction with other powers*" refers to the use of the powers under the Terrorism Act 2000 together with powers under various other legislative provisions, such as the Misuse of Drugs Act 1971.

	Section 43	**Section 43A**	**Section 43/43A**	**Section 47A**	**TACT in conjunction with other powers**	**Section 21 JSA**	**Section 24 JSA**	**Sections 21/24 JSA**
2014	77	4	15	0	18	1301	3660	563

[546] Professor Marie Breen-Smyth, First Report, 5.3-5.5.
[547] Comparing the period August 2020 to July 2021, against the period August 2019 to July 2020.
[548] Figures provided to me by PSNI Statistics Branch.

2015	105	13	78	0	38	1307	4384	619
2016	91	11	92	0	34	1783	7285	986
2017	65	3	29	0	13	1163	6109	610
2018	41	2	9	0	13	1023	6052	323
2019	26	4	8	9	5	920	5003	189
2020	22	1	4	0	3	361	3519	128
2021	22	4	2	0	7	416	3588	79

9.20. Unlike in Great Britain, the self-defined ethnicity of those stopped in Northern Ireland is not recorded or published (only the officer-perceived ethnicity of individuals stopped and searched is recorded[549]).

9.21. In 2021 the number of stops carried out under section 43 of the Terrorism Act 2000 was the same as it was last year. This is in the context of a 76% decline in the number of stops carried out under section 43 since 2016.

9.22. In terms of the community monitoring mandated by the Northern Ireland Court of Appeal's judgment in *Ramsay (No. 2)*[550] to which I have referred in my previous two reports, Professor Marie Breen-Smyth reports that the PSNI has yet to settle on a methodology for conducting community monitoring. Professor Breen-Smyth states that the PSNI has assured her that they are committed to implementing community background monitoring of the stop and search powers contained in the Justice and Security (Northern Ireland) Act 2007.[551] She has made several recommendations intended to expedite the commencement of community monitoring.[552]

9.23. The Northern Ireland Policing Board has argued for community monitoring in the context of the powers in the Terrorism Act. I have expressed scepticism in the past about the value of community monitoring in the Terrorism Act context, given that it is used almost exclusively against dissident republicans. However, I will avoid drawing any firm conclusions until the PSNI collects the relevant data.

Cordons

[549] Para 4.3(x) Police & Criminal Evidence (Northern Ireland) Order 1989 Code A.
[550] In the matter of an application by Stephen Ramsey for judicial review (No. 2) NICA 14.
[551] Professor Marie Breen-Smyth, First Report, para 6.96.
[552] Ibid, at para 6.101.

9.24. The following table sets out the number of designated cordons in place in each year since the Terrorism Act 2000 was enacted.[553] There has been a significant decline in the use of cordons in Northern Ireland.

Year	Number of designated cordons
2001	62
2002	239
2003	175
2004	126
2005	72
2006	38
2007	29
2008	59
2009	102
2009/10	128
2010/11	120
2011/12	87
2012/13	57
2013/14	55
2014/15	45
2015/16	43
2016/17	29
2017/18	16
2018/19	18
2019/20	17
2020/21	20
2021/22	6[554]

Arrest and Detentions

9.25. The powers of arrest in section 41 of the Terrorism Act 2000 are set out in Chapter 5. In Northern Ireland, there were a total of 130 arrests made under section

[553] Northern Ireland Office, 'Northern Ireland Terrorism Legislation: annual statistics 2021/22, Table 10.1.
[554] Police Service of Northern Ireland (provided as unvalidated management information sourced from administrative systems). Future publications of cordon data will now run on a calendar year basis.

41 of the Terrorism Act 2000 in 2021 (51 more than in the previous year).[555] This was the highest number of arrests made under section 41 since 2019. Nevertheless, the trend overall is that section 41 is being used much less frequently by the PSNI than it was in the past.

9.26. I pointed out last year that the official PSNI statistics for the use of section 41 relate to the "security situation" only, therefore to Northern Ireland-related terrorism, whereas persons who have been arrested under section 41 for other reasons are excluded.

- I recommended that that PSNI's published statistics should include all arrests under section 41.
- However, my recommendation was rejected by the Chief Constable of the PSNI on the basis that statistics published by the Northern Ireland Office includes data on all arrests under section 41, even though the PSNI's statistics do not.
- I recognise the force of the Chief Constable's point that PSNI's statistics are specifically directed to the "security situation". It is to be hoped that statistics on the use of terrorism powers can be normalised in due course, because I remain of the view that PSNI should publish all section 41 arrests (if necessary, distinguishing between those relating to, and not relating to, the "security situation") in the interests of improving transparency of and accountability for the use of this strong power.

9.27. As with previous years, Northern Ireland accounted for a very high proportion of the arrests made under section 41 of the Terrorism Act 2000. In Great Britain there were 32 arrests during 2021[556]. This year the Northern Ireland figure was 80 % of all section 41 arrests in the United Kingdom (last year it was 75%). This is a trend that I have sought to understand.

9.28. My understanding is that the PSNI takes the view that arrests for terrorist-related activity ought to be carried out using terrorism powers for reasons relating to public perception[557]. In last year's report, I recommended that the PSNI should not

[555] PSNI, 'Policing Recorded Security Situation Statistics for Northern Ireland', Table 5.
[556] Home Office, 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation, year ending December 2021', Table A.01.
[557] Terrorism Acts in 2020 at 9.36.

take account of public perception when deciding on the appropriate arrest power for terrorist-related activity.

- In his response to that recommendation, the Chief Constable acknowledged the difference in relative reliance on section 41 between Great Britain and Northern Ireland and referred to the need for PSNI to police in a manner that secures the support and confidence of the community (see section 31A of the Police (Northern Ireland) Act 2000).
- Although he rejected my recommendation, the Chief Constable referred to further engagement with me on this issue, which I look forward to during the coming year.

9.29. Of the 130 people detained under section 41 of the Terrorism Act 2000, there were 3 applications for warrants of further detention and no refusals[558].

9.30. The 130 arrests made under section 41 resulted in 23 people being charged with an offence. This represents a charge rate of 18 % (the same figure as last year).

9.31. There can be no doubt that the charge rate in Northern Ireland following arrest under section 41 is anomalous when compared with that in Great Britain. In the year under review the charge rate in Northern Ireland was 18 % while in Great Britain it was 69 %. In preparing last year's report, I was informed that the PSNI intended to commission a working group to review current practices on the use of section 41 of the Terrorism Act 2000. I have not heard anything further about this but hope that it can be considered in the coming year in line with the Chief Constable's commitment to engage with me on the public perception aspect of section 41.

Conditions of detention

9.32. Independent Custody Visitors in Northern Ireland are trained and coordinated by the Northern Ireland Policing Board. Unlike in Great Britain, there is no statutory requirement in Northern Ireland for custody visitors' reports to be sent to me, but in practice they are.

[558] Northern Ireland Office, 'Northern Ireland Terrorism Legislation: annual statistics April-December 2021', Table 3.1.

9.33. The outcome of the Northern Ireland Policing Board's review of custody visiting forms is awaited. Comparing a visit report dated 29 June 2022 with one dated 3 June 2019, I can say that the same form is still being used that I commented on in my first report[559].

9.34. The table below sets out information provided to me by the Policing Board of Northern Ireland about the independent custody visits which took place in Northern Ireland in 2021. All detainees were arrested under section 41 Terrorism Act 2000.

2021	Detainees	Valid visits	Invalid visits	Seen by ICVs	CCTV reviews	Unsatisfactory visits
	87	43	6	36	7	0

Stopping the Travelling Public

9.35. Schedule 7 of the Terrorism Act 2000 allows officers to examine those travelling through ports or borders to determine if they are terrorists; to search them; to detain them; to require them to hand over electronic devices for examination; and to take their fingerprints. Failure to cooperate with an examination is a criminal offence.

9.36. As in Great Britain, there has been a decline in the number of Schedule 7 examinations in Northern Ireland.

Year	Number of stops
2016	2082
2017	1248
2018	717
2019	559
2020	120[560]
2021	139

[559] Terrorism Acts in 2018 at 9.72.
[560] This is a revised figure for 2020 provided to me by PSNI Statistics Branch (up from 119).

9.37. In terms of detentions, in 2017, 11 people were detained. In 2018, 6 people were detained. In 2019, 31 people were detained. In 2020, 11 people were detained[561]. In the year under review 34 people were detained.

9.38. As with previous years, I obtained the figures in self-defined ethnicity directly from the PSNI as they are not published.

Total examinations

	2020	**2021**
White	38%	41%
Mixed	8%	6%
Black	13%	10%
Asian	17%	20%
Chinese or other	16%[562]	16%
Not stated	8%	6%

Detentions

	2020	**2021**
White	0%	26%
Mixed	18%	9%
Black	27%	9%
Asian	27%	24%
Chinese or other	9%	24%
Not stated	18%[563]	9%

9.39. In terms of freight, in the year under review there were 19 examinations of unaccompanied freight (in 2020 there were also 19).

[561] Revised figure for 2020 (up from 8).
[562] PSNI Statistics Branch have revised the figures for Asian and Chinese or other people who were examined: the previous figures given were 16% and 17% respectively. During 2020 there were also a small number of ethnicity returns that were not completed.
[563] The detention figures have also been revised. The number of detentions is low (11) so 27% equates to 3 people detained.

Brexit

9.40. The transition period ended on 31 December 2020. The year under review saw the coming into force of the Northern Ireland Protocol requiring certain goods travelling between Great Britain and Northern Ireland to be checked upon entering Northern Ireland. This led to significant discontent in the loyalist community, although it did not produce the levels of violence that had been feared. In 2021 the Loyalist Communities Council and the Progressive Unionist Party, the political wing of the Ulster Volunteer Force, withdrew their support for the Belfast/Good Friday Agreement as a result of opposition to the Protocol. Between April and May serious disorder resulted in the deployment of water cannon and public order dog teams. For the first time in 3 years, the PSNI discharged rounds of Attenuating Energy Projectiles. Over 100 police officers were injured during this disorder. As the year progressed, public disorder subsided, although there were localised incidents at times of increased tension. So far, protests of this nature have been dealt with using public orders powers.

Terrorist Trials, Sentencing, and Criminal Justice

9.41. I agree with the view attributed to MI5 by the Intelligence and Security Committee of Parliament in 2019[564] that criminal justice outcomes are the preferred course of action in the terrorism context wherever possible, as they are a critical tool to successful and long-term disruption. In each my three previous reports, I have remarked that the slow pace and procedural heaviness of criminal proceedings in Northern Ireland has a deleterious impact on the use of terrorism legislation. I am afraid to report that very little progress has been made to improve the situation.

9.42. Turning first to delay, in my previous three reports I have drawn attention to the issue of oral committal hearings and proposals for their reform. I am pleased to report that the Criminal Justice (Committal Reform) Bill was granted Royal Assent in 2022. However, as I remarked last year,[565] the legislation adopts a phased approach that will not impact offences of the sort typically committed by terrorists (such as weapons training and collecting information likely to be of use to a terrorist). Committal hearings

[564] Intelligence and Security Committee of Parliament, Northern Ireland-related Terrorism, HC 844 (5 October 2020).
[565] Terrorism Acts in 2020, paras 9.69-9.72.

have therefore been abolished for some terrorism offences, but not others. This is regrettable. The other source of delay I have remarked upon concerns the lack of robust case management powers in the Northern Ireland Crown Court.[566] I am afraid to say that no discernible progress has been made to address this problem.

9.43. In terms of sentencing[567], it is now generally accepted that sentences for terrorism offences in Northern Ireland are lower than they are in England and Wales. As I explained last year,[568] there appears to be no appetite in Northern Ireland for the creation of a guideline body akin to those established in England and Wales and Scotland. In the absence of such a body, I saw no reason of principle why the relevant guidelines from England and Wales should not be taken into account when sentencing terrorism cases in Northern Ireland.

9.44. To achieve greater consistency in terrorism sentencing between Northern Ireland and the rest of the United Kingdom, last year I recommended that the Director of Public Prosecutions for Northern Ireland seek an authoritative ruling from the court on whether the terrorism sentencing guidelines issues by the Sentencing Council for England and Wales or the Scottish Sentencing Council should be considered for the purpose of sentencing terrorism cases in Northern Ireland.

- I am pleased to report that in R v Niall Lehd [2022] NICA 51, the Court of Appeal in Northern Ireland held that when sentencing cases of attack-planning contrary to section 5 Terrorism Act 2006, judges in Northern Ireland were not bound to apply, but were at liberty to consider, the Sentencing Council of England and Wales' guidelines on the offence. This could assist them in identifying aggravating and mitigating facts and features, and by suggesting sentencing ranges as "an aid to orientation"[569].

[566] Ibid, para 9.72
[567] In R v Morgan and others [2021] NICA 67 the Court of Appeal (Northern Ireland) held that retrospective changes to the release provisions of serving prisoners (made under the Counter-Terrorism and Sentencing Act 2021), did contravene Article 7 ECHR, and granted a certificate of incompatibility. The opposite result had been reached in England and Wales in R (Khan) v Secretary of State for Justice [2020] 1 WLR 3932. The difference was accounted for by the different role of the sentencing judge in Northern Ireland (Morgan, para 86).
[568] Ibid, para 9.75.
[569] At para 89.

10. **SCOTLAND**

10.1. The Terrorism Acts apply to Scotland because national security and special powers for dealing with terrorism are reserved matters under the Scotland Act 1988[570]. Their operation in practice is modified somewhat by Scotland's different legal system and the relationship between the Lord Advocate and Police Scotland[571].

10.2. The most serious terrorism prosecution in Scotland in 2021 was the case of Sam Imrie. The Extreme Right Wing Terrorist was sentenced to 7 and a half years' imprisonment in December 2021 for encouraging terrorism and having possession of information likely to be useful to a terrorist[572], together with offences of wilful fire-raising, drink-driving and possession of child sex abuse material[573].

- He was charged with attack planning, in relation to threats to livestream an attack on an Islamic Centre in Fife, but acquitted.
- Imrie was a socially-isolated individual who had stockpiled a number of weapons.
- He had possession of copies of manifestos by New Zealand attacker Brenton Tarrant and Anders Brievik.

10.3. In September 2021, two boys (15 and 16) were convicted of encouragement, dissemination, and possession of useful material[574] and sentenced to a 2 year youth rehabilitation and 3 year crime behaviour order, and 12 month intensive referral order respectively.

10.4. Despite this, and possibly because Scotland has a lower CT caseload, the same patterns of youth offending as exist in England and Wales have not become apparent, although there are increasing incidents of neurodiversity and poor mental health.

10.5. If Police Scotland and the Crown Office and Procurator Fiscal Service do encounter an increase in juvenile offending (and associated issues such as modern

[570] Schedule 5 Part II para B8.
[571] Described in Terrorism Acts in 2019 at 10.6 to 10.15.
[572] Section 1 Terrorism Act 2006, section 58 Terrorism Act 2000.
[573] 'Man jailed for threatening to burn down mosque' (BBC News, 2.12.21).
[574] Sections 1, 2 Terrorism Act 2006, section 58 Terrorism Act 2000: in Chapter 7 I refer to these as the 'information offences'.

slavery) as in England and Wales, it will be informative to see how Scotland's different legal and social work systems[575] respond to the phenomenon, and whether there are lessons which can be applied elsewhere in the United Kingdom.

10.6. At the other end of the age spectrum, in September 67-year old Firoz Madhani was convicted before Edinburgh Sheriff Court of encouraging terrorism online and was sentenced to 8 months' restriction of liberty (a form of house curfew) and placed under supervision for a year[576].

10.7. The National Preventive Mechanism released its annual report on the monitoring of places of detention during Covid[577] including persons detained under section 41[578]. Some in-person visits elsewhere continued in the UK, and the Home Office and the Independent Custody Visitors Association developed workarounds such as remote monitoring of people in custody, but Scotland was something of an outlier. The report notes that the Scottish government did not provide independent custody visitors with the same level of support and visiting ceased in March 2021[579].

10.8. In Chapter 4, I have drawn attention to some features of investigating online terrorism based on my discussions with CT Police operating in England and Wales. I accept that Police Scotland, with its lower CT caseload, may not have found these features to be of prominence, but, because it concerns legality, I would encourage Police Scotland to consider Chapter 4's analysis on:

- Remote access.
- Retention and deletion of electronic data.
- Unexpected discovery of legally privileged material on seized devices.

10.9. I look forward to reporting on how Police Scotland deal with these matters in next year's report. As with Police Scotland's useful guidance on 'Auditors'[580], it is possible that there are points of learning between the nations of the UK.

[575] For example, the Scottish Children's Reporters Administration.
[576] 'Man published tweets encouraging terrorism against India' (COFPS, 16.11.21).
[577] 12th Report of the National Preventive Mechanism, CP 607 (February 2022).
[578] The Criminal Legal Aid and Advice and Assistance (Counter-Terrorism and Border Security) (Scotland) Regulations 2021 SSI 2021/55 extend the class of person for whom the Scottish Ministers may make automatic, non-means tested criminal legal advice and assistance available, to include where a person is detained under section 41 or schedule 7 of the Terrorism Act.
[579] Ibid, at page 17.
[580] See Chapter 4.

11. **ONLINE RADICALISATION**

11.1. In this chapter, I review the topic that garners continuing attention in the field of terrorism studies: online radicalisation. I then consider the fundamental values that are at stake when online content is moderated in the name of terrorist risk reduction.

11.2. I refer to online radicalisation as a species of persuasion whose destination is an act of terrorism as defined by the Terrorism Act 2000, rather than the mere development of extreme beliefs[581].

- One of my predecessors wisely observed that just because extremism is a word does not mean that it is a legally useful concept[582], and as the government has found, extremism has proven impossible to define[583].
- Countering online content on the basis that it may lead to terrorist violence is one thing[584], but doing so on the basis that it may lead to extremism is quite another.

11.3. However, it is impossible to avoid the word "extremist" in the literature on online radicalisation, and I occasionally use the word, with the caveat that the remit of this report is counter-terrorism not counter-extremism.

11.4. I refer to counter-terrorism but there may be other national security interests in play: in 2022, the Intelligence and Security Committee of Parliament heard some evidence of Russian state support for some extreme right wing groups in order to fuel divisions in the UK[585]. It is therefore possible that removing radicalising content may be desirable for other national security reasons.

The phenomenon

[581] Stuart MacDonald and Joe Whittaker have pointed to a serious lack of clarity in the use of terms such as radicalisation, online radicalisation and self-radicalisation: Macdonald, S. & Whittaker, J. (2019). Online Radicalization: Contested Terms and Conceptual Clarity. John R. Vacca (Ed.), Online Terrorist Propaganda, Recruitment, and Radicalization, Boca Raton: CRC Press.
[582] Lord Anderson QC, 'Extremism and the Law', Treasurer's Lecture, Middle Temple Hall (18.3.19).
[583] See 'Operating with Impunity' (February 2021), for a recent attempt by the Commission for Countering Extremism.
[584] Some take the view that expression of radical reviews is no predictor of future violence at all: Faure Walker, R., 'The Emergence of 'Extremism': Exposing the Violent Discourse and Language of 'Radicalisation' (Bloomsbury, 2021).
[585] ISC, 'Extreme Right Wing Terrorism', supra, at para 129.

11.5. The forensic psychiatrist, terrorism scholar, and former CIA officer, Marc Sageman is credited with identifying features of the internet that altered the nature of terrorist radicalisation: heightened vitriol, polarising of groups and non-hierarchical structures[586].

11.6. Government policy is conducted on the broad premise that the internet content increases the likelihood of terrorism by persuading people to commit acts that they would not otherwise perform[587].

11.7. Terrorism scholars have offered various descriptions of how the internet provides several functions and mechanisms that allow for online interaction, including in the absence of actual social interaction[588], and drawing on "online disinhibition"[589].

11.8. They also point out that:

- The internet is not a single entity; platforms (such as Facebook or Twitter or 4Chan) operate very differently from one another (referred to as "affordances") and result in markedly different radicalising behaviours.
- Radicalisation often has a social dynamic, which is at odds with the popular image of passive consumption of content[590].
- Indeed, it has been argued that 'online radicalisation' is a misnomer which suggests a false dichotomy between the online and offline worlds[591], and a broader view should be taken of the internet's responsibility for terrorist

[586] Sageman, M., 'Leaderless jihad: Terror networks in the twenty-first century' (University of Pennsylvania Press, 2008).
[587] HMG, Impact Assessment, Online Safety Bill (31.1.22) at para 320: although "it is hard to quantify the benefit of the removal of terrorist content and activity from the online sphere", removal "will almost certainly have an effect on the level of terrorism in society".
[588] Binder, J., Kenyon, J., 'Terrorism and the internet: How dangerous is online radicalization?' (2022) Front. Psychol. 13:997390.
[589] For example, Molmen, S., 'Mechanisms of online radicalisation: how the internet affects the radicalisation of extreme-right lone actor terrorists' (2021) Behavioral Sciences of Terrorism and Political Aggression, proposes 6 mechanisms for this type of terrorism: compensation for offline weaknesses; countering social isolation, facilitation, acceleration, echoing, and violent action triggering. Many of the theoretical bases for radicalisation are summarised in Whittacker, J., 'Rethinking Online Radicalisation', Perspectives on Terrorism (2022), vol.16, issue 4.
[590] 'Determining the role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', Studies in Conflict in Terrorism Vol. 40 (2017).
[591] Whittacker, J., supra; Kanol, E., 'Contexts of Radicalization of Jihadi Foreign Fighters from Europe' (2022) 16.3 Perspectives on Terrorism 45.

violence relative to family influence, friendship groups, real world interactions, neurodivergence and mental health[592].

- Internet use is constantly changing over time and may affect different groups differently[593]. Online radicalisation in the context of those who travelled from the UK to Syria and Iraq to join Islamic State between 2013 and 2016 is likely to differ from its impact on young people during and after the Covid-19 pandemic. Studies may become quickly outdated[594].
- Radicalisation could in principle be achieved by algorithmic promotion of certain content[595] without a human radicaliser at the other end[596]. The consequences of recommendation systems have been strikingly illustrated in relation to TikTok and the extreme right[597].

11.9. It is fair to say much theoretical analysis of online radicalisation is based on no or limited empirical research. Researchers lack ready access to terrorists and secret intelligence, and in any event the sample size is small, their focus is more often on the supply side of internet propaganda (actors[598], contents[599], platforms and

[592] E.g. Hamid, N., Ariza, C., 'Offline Versus Online Radicalisation: Which is the Bigger Threat?' (GNET, King's College London, 2022); Herath, C., Whittaker, J., (2021) 'Online Radicalisation: Moving beyond a Simple Dichotomy', Terrorism and Political Violence. Having regard to Kenyon's research, see below, I believe this overstates the point.

[593] Moskalenko, S. Gonzales, J., Kates, N., Morton, J., 'Incel Ideology, Radicalisation and Mental Health: A Survey Study', Journal of Intelligence, Conflict, and Warfare, Vol4 Issue3 (2021) finds that incels used a diverse and rapidly evolving range of platforms from mainstream and alternative online forums like Reddit, 4chan, 8Chan and 8Chan to chat rooms dedicated to online gaming such as Discord.

[594] As recently as 2013, a study noted a consensus that self-radicalisation is extremely rare, if possible at all: Von Behr, I., Reding, A., Edwards, C., Gribbon, L. **'**Radicalisation in the digital era : the use of the internet in 15 cases of terrorism and extremism'(RAND Europe.; Rand Corporation, 2013.)

[595] E.g., those used in Youtube's recommendation system described by Goodrow, C., 'On Youtube's recommendation system', YouTube Official Blog (15.9.21). Indeed, victims of international terrorism have recently argued that Facebook should incur civil liability on the basis that its "friend suggestion" connects radicalised users to terrorist groups like Hamas: Yost, E.S., Social support for terrorists (2021) 37 Santa Clara High Technology Law Journal 301.

[596] Although artificial intelligence may, like anything else, be used maliciously: UN Office of Counter-Terrorism, 'Algorithms and Terrorism: the Malicious Use of Artificial Intelligence for Terrorist Purposes' (2021).

[597] Little, O., Richards, A., 'TikTok's algorithm leads users from transphobic to far-right rabbit holes', Los Angeles Blade (11.10.21). However, there may be insufficient evidence to support claims of radicalisation by algorithm, Whittacker, J., 'Recommendation Systems and Extremism: What do we Know?', GNET Insights (17.8.22).

[598] Such as committed group members (cf. Tech Against Terrorism, 'The Threat of Terrorist and Violent Extremist-Operated Websites' (2022)), or unaffiliated supporters such as 'jihobbyists' (Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., Weir, D.,'Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts', Studies in Conflict & Terrorism (2019), 42:1-2, 141-160).

[599] For example, Davey, J., Comerford, M., Guhl, J., Baldet, W., Colliver, C., 'A Taxonomy for the Classification of Post-Organisational Violent Extremist and Terrorist Content', Institute for Strategic Dialogue (2021) identify 3 overarching categories: inspirational, ideological and instructional.

techniques[600]) rather than audience engagement (its effect on terrorist offending)[601]. It has proven difficult to observe mainstream analytical frameworks in the data[602].

11.10. The Ministry of Justice has now sponsored research based on the risk assessments (known as "ERG 22+") of terrorist offenders in the UK[603]. I have already referred to this research in Chapter 5 in the context of (i) mental health and neurodivergence and (ii) risk.

11.11. Unsurprisingly this research found that the internet has been an important, and ever increasing means of radicalisation and, in the period 2019 to 2021 (coinciding with the Covid pandemic, although possibly just reflecting the ever-increasing use of the internet across society) was the primary means of radicalisation (59% of cases).

11.12. Female terrorists and older terrorists were found to be catching up on internet radicalisation with younger terrorists, whose exposure and susceptibility to terrorist-related material has been well-documented[604].

Causes

11.13. Becoming radicalised implies the acceptance of reasonably coherent beliefs calling for fundamental social change, or adherence to a group or party with a distinct if extreme position[605]. Terrorism requires the use or threat of violence "for the purpose of advancing a political, religious, racial or ideological cause"[606].

11.14. Few difficulties are presented by Islamic State or Al Qa'eda- produced content. Salafi-jihadism is a vital motivating force for much of what is referred to as Islamist

[600] E.g. Macdonald, S., Rees, C., S., J., 'Remove, Impede, Disrupt, Redirect: Understanding and Combating Pro-Islamic State Use of File-Sharing Platforms' (Resolve Network, April 2022); Michael Zekulin (2021) From Inspire to Rumiyah: does instructional content in online jihadist magazines lead to attacks?, Behavioral Sciences of Terrorism and Political Aggression, 13:2, 115-141.
[601] The lack of interviews represents a serious impediment to effective research: Christmann, K., 'Preventing Religious Radicalisation and Violent Extremism: A Systematic Review of the Research Evidence' (Youth Justice Board, 2012).
[602] Bouhana, N., Schumann, S, 'Are Conceptual Frameworks of Radicalisation Leading to Involvement in Terrorism 'Observable'?', Crest (March 2022).
[603] Kenyon, J., Binder, J. F., & Baker-Beall, C., Ministry of Justice Analytical Series (2022).
[604] E.g. Rose, R., AC, ' "We are Generation Terror!": Youth-on-Youth Radicalisation in Extreme-Right Youth Groups' ISCR (2021).
[605] New Shorter Oxford English Dictionary, "Radical: Radical: advocating thorough or far-reaching change; representing or supporting an extreme section of a party".
[606] Section 1(1)(c) Terrorism Act 2000.

terrorism[607]. The current wave of Islamist ideology underpinning attacks over the last two decades has at least this dubious advantage: it is in the main recognisable.

11.15. Diversity within the jihadist spectrum has in the past been explained in terms of different groups with varying regional or local preoccupations, with real world fluidity between groups occurring for strategic, logistical, or financial reasons rather than ideological ones [608]. However, fragmentation along strategic or ideological lines should not be ignored: jihadi activity and beliefs are not monolithic

11.16. But much current terrorism research, as well as coverage of the government's Prevent scheme, is concerned with the amorphous category of 'mixed, unstable and unclear ideology'. According to this this research, captured within the 'far right' can be a range of different and new-fangled "flavours" including violent incel ideology and non-ideological school shooting[609]. In the online setting these flavours are often found mixed in the same pot.

- Practitioners have noted a "proliferation and confusion of ideologies" on the far right[610]. The Director of the FBI referred recently to 'salad-bar' extremism (the phrase Pick 'n' Mix is used on this side of the Atlantic)[611], although this suggests a process of intentionally picking and mixing beliefs to fit personal outlook which sounds too deliberate[612].

- It is therefore now common to refer to a "fractured" right wing terrorist scene[613], where movements and groupuscules "mobilise around a wide range of

[607] El-Badawy, El, Comerford, M., Welby, P., 'Inside the Jihadi Mind: Understanding Ideology and Propaganda' (Tony Blair Institute for Global Change, 2015).
[608] Wright, R., et al, 'The Jihadi Threat: ISIS, Al Qaeda and beyond' (United States Institute of Peace, Wilson Centre, 2017).
[609] Brace, L., 'A Short Introduction to the Involuntary Celibate Sub-Culture' (CREST, 26.8.21).
[610] Pantucci, R., and Ong, K., 'Persistence of Right-Wing Extremism and Terrorism in the West' (International Centre for Political Violence and Terrorism Research, 2021). In the right wing context (but not exclusively) it is common to discuss 'narratives' (plural): e.g. 'Radical Right Counter Narratives Project' (Expert Workshop Report, Hedayah & CARR, 2019). See Lee, B., 'A Short Guide to Narratives of the Far-Right' (Crest, 1.6.20).
[611] E.g. Dryden, M., 'An Ideological Pick 'n' Mix: The Rise of 'Mixed' Ideologies and their implications for Terrorist Violence', HJS Centre of Radicalisation and Terrorism (March 2021).
[612] Instead, ideologies may emerge non-linearly from an amalgamation of inputs and feedback loops facilitated by social media and other platforms: 'Will 'Salad Bar Extremism' Replace 'Old-School World' Terrorism', the National Interest (14.7.22).
[613] Hoffman, B., Ware, J., 'The Terrorist Threat from the Fractured Far Right' (Lawfare, 1.11.20).

different ideologies, grievances and modes of action" [614] . Common preoccupations may surface leading to ideological "convergence" [615]. They may be part of a movement or network[616], brand[617], or wave[618]. Looseness has been perceived as a weakness on the part of right wing terrorists, hence recent attempts to build coalitions across ideologically aligned individuals[619].

- In terms of UK classification, some preoccupations would be seen as falling outside Extreme Right-Wing Terrorism. For example, incel-promoting violence could fall within Left, Anarchist and Single Issue Terrorism ('LASIT'), whilst the desire to perpetrate a school shooting could fall outside the definition of terrorism all together[620].

11.17. Of course, crude contrasts between coherent Islamism and incoherent Right Wing Terrorism should be avoided. Neo-Nazi ideology has a long pedigree and the programme of proscribed groups such as National Action is no less coherent an ideology than Islamist terrorism. Many contemporary extreme right wing groups are anchored to a single text: James Mason's Siege[621].

11.18. Moreover, some of the apparent difficulty in pinpointing a coherent set of beliefs behind an online call to violence may be down to novelty and the time required for practitioners to catch up. If the history of terrorism shows anything it is that unexpected ideologies may prove the catalyst the violence, from the Red Army Faction and Red

[614] Allchorn, W., 'From Street-Based Activism To Terrorism & Political Violence: Uk Radical Right Narratives & Counter- Narratives At A Time Of Transition', Hedayah & Centre for Analysis of the Radical Right (2021)
[615] Hoffman, B., Ware, J., 'The Challenges of Effective Counterterrorism Intelligence in the 2020s' (Lawfare, 21.6.20).
[616] Upchurch, H., 'The Iron March Forum and the Evolution of the "Skull Mask" Neo-Fascist Network', CTC Sentinel 14:10 (2021).
[617] Koehler, D., 'When branding turns toxic: a theoretical framework for modern extreme-right brand networks', Behavioral Sciences of Terrorism and Political Aggression (2022).
[618] Auger, Vincent A. "Right-Wing Terror: A Fifth Global Wave?" Perspectives on Terrorism 14, no. 3 (2020): 87–97.
[619] Shadnia, D., Newhouse, A., Kriner, M., Bradley, A., 'Militant Accelerationism Coalitions: A Case Study in Neo-Fascist Accelerationist Coalition Building Online' (Tech Against Terrorism & Centre on Terrorism, Extremism, and Counterterrorism, 2022).
[620] See further, Terrorism Acts in 2019 at 2.32.
[621] Johnson, B., Feldman, M., 'Siege Culture after *Siege*: Anatomy of a Neo-Nazi Terrorist Doctrine', ICCT (July 2021).

Brigades of 1960s[622] to, perhaps in the future, eco-terrorism[623], Anti-vax or QAnon[624]. Unfamiliarity does not equate to incoherence.

11.19. Nonetheless, the category of potentially radicalising material goes well beyond propaganda produced by established terrorist organisations or supporting established ideologies.

Real World Violence

11.20. The chief object of counter-terrorism is to safeguard the population from acts of violence done to pursue a political, religious, racial, or ideological programme and their wider impact. Physical violence does not take place in cyberspace, so online radicalisation concerns online content or behaviour that might lead to real world violence on some subsequent occasion.

11.21. However, no content automatically radicalises, let alone leads to violence[625], because the most people will respond to terrorist propaganda with aversion, and even showing a link between the publication of instructional material and violence is complex[626]. Nor can it be said that potentially radicalising material is inherently wrong, like child sex abuse material.

11.22. Context as well as content is relevant[627]. It is plausible that promoting 'the great replacement theory' on a forum devoted to violent resistance against non-Whites has greater radicalising potential than sharing it during a discussion of the French presidential election or Fox News[628]. The identity of the speaker may be high

[622] Burleigh, M, 'Blood and Rage: a Cultural History of Terrorism', supra.
[623] Farrell-Molloy, J., Macklin, G., 'Ted Kaczynksi, Anti-Technology Radicalism and Eco-Fascism' (ICCT, 15.6.22).
[624] In June 2021, the FBI assessed that some violent adherents of QAnon would start engaging in real world violence: 'Adherence to QAnon Conspiracy Theory by Some Domestic Violent Extremists' (4.6.21). Aboudouh, A., 'Unparalleled threats: Anti-vaxxer movement threatens a new wave of extremism' (Independent, 19.1.22).
[625] Graham Smith makes the powerful point that online speech should not be regarded as inherently risk-creating in 'Speech is not a tripping hazard – response to the Online Harms White Paper' (28.6.19).
[626] Zekulin, M., 'From Inspire to Rumiyah: does instructional content in online jihadist magazines lead to attacks?', (2021) Behavioral Sciences of Terrorism and Political Aggression, 13:2, 115-141.
[627] Cf the UN Office of High Commissioner of Human Rights' Rabat threshold test. Decisions on whether speech contravenes Article 20 ICCPR (incitement to hatred) should take account of (1) the social and political context, (2) status of the speaker, (3) intent to incite the audience against a target group, (4) content and form of the speech, (5) extent of its dissemination and (6) likelihood of harm, including imminence.
[628] Rose, S., 'A deadly ideology: how the 'great replacement theory' went mainstream (Guardian, 8.6.22).

pertinent: a study of material found in cases of Islamist terror attacks found that even moderate sermons by Anwar Al-Awlaki were sought out by the attackers[629].

11.23. It is not only degenerate content that has the capacity to radicalise to violence. Extracts from the Qu'ran are used to exhort terrorist killings[630]. A BBC3 documentary appears to have radicalised Darren Osbourne, who carried out a terrorist attack on worshippers at Finsbury Park Mosque in 2017[631].

- There is no definition that can capture material that has the capacity to radicalise, but is otherwise worthy of protection for journalistic, cultural, religious, topical, comedic or other reasons. Nasheeds, even 'jihadi nasheeds' (which have something in common with drill music), are problematic for this reason[632].
- There is no reason why tech companies should be any better at deciding worth than anyone else.

11.24. A further complexity is that explicitly terrorist material may be collected and exchanged for obscure reasons (for example, a love of 'gore') that have nothing to do with terrorism[633].

11.25. Assuming that physical violence is the right metric for considering online radicalisation opens up the following issue of fundamental relevance: the eyeballs to violence ratio, that is, the relationship is between the number of eyeballs on enabling or inspiring content, and the number of terrorist plots or attacks during the same period. No attempts have been made to quantify this, but one can be confident that

[629] Holbrook, D., 'What Types of Media do Terrorists Collect?' (International Centre for Counter-Terrorim, The Hague, 2017).
[630] Holbrook, D., Using the Qur'an to Justify Terrorist Violence: Analysing Selective Application of the Qur'an in English-Language Militant Islamist Discourse, Perspectives on Terrorism Vol.4 Issue 3 (2010).
[631] Glazzard, A., Shooting the Messenger: Do Not Blame the Internet for Terrorism, RUSI Newbrief, vol 39 issue 1 (2019); Dodd, V., 'How London mosque attacker became a terrorist in three weeks', Guardian (1.2.18).
[632] Henrik Gråtrud (2016) Islamic State *Nasheeds* As Messaging Tools, Studies in Conflict & Terrorism,39:12, 1050-1070.
[633] E.g., individuals who collect and disseminate Islamic State videos as a species of online 'gore'. In 'The Coming Storm' (BBC Radio 4, Dec 2021-Feb 2022), Gabriel Gatehouse described the competitive instinct on websites such as 4Chan and 8Chan to invent attention-grabbing memes to get one's content to the top of the list.

that it is only an exceptionally small subset of consumers who will then go on to use violence[634].

- For a sense of scale, there were 1.5 million video uploads of the Christchurch live-stream in the first 24 hours after the 2019 attack[635]. Assuming some degree of automation, and numerous uploads by the same individuals, this suggests a figure of hundreds of thousands of people exposed to this content, which is still available on platforms today.
- A recent analysis of 33 terrorist-operated websites (including both Islamist and Extreme Right Wing) found 1.54 million monthly visits[636].

11.26. Academics describe this as the "specificity problem": the fundamental question as to why only a few people carry out violence when so many appear to have been exposed to at least some of the same causes of radicalization[637].

11.27. In short, to wish restrictions on the internet freedoms of millions and billions of users, based on the violent actions of the spectacular few[638], seems an unnecessarily heavy price to pay, akin to banning knives or alcohol [639].

11.28. In an ideal world, therefore, governments would manage the risks posed by violent individuals, leaving the internet as a neutral ground for free expression by the

[634] For a sense of scale, there were 1.5 million video uploads of the Christchurch live-stream in the first 24 hours after the attack: New Zealand Government, 2021 Digital Violent Extremism Report (at p31). Assuming some degree of automation, and numerous uploads by the same individuals, this suggests a figure of 100s of thousands exposed to this content, which is still available on platforms today (ibid). Berger, J.M., Perez, H., 'The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters', occasional paper, GW Program on Extremism (2016) contains an analysis of IS Twitter supporters June to October 2015. Tech Against Terrorism, 'The Threat of Terrorist and Violent-Extremist Operated Websites' (January 2022), found that a sample of 33 out of 198 identified websites had 1.54 million monthly visits.

[635] New Zealand Government, 2021 Digital Violent Extremism Report (at p31)

[636] Tech Against Terrorism, 'The Threat of Terrorist and Violent-Extremist Operated Websites' (January 2022).

[637] See for example, Ylitalo-James, E., & Silke, A., 'How Proximity and Space Matter: Exploring Geographical & Social Contexts of Radicalization in Northern Ireland', (2022) Studies in Conflict & Terrorism; Derfoufi, Z., 'Radicalization's Core', Terrorism and Political Violence, (2022) 34:6, 1185-1206.

[638] To use the phrase coined by Mark Hamm for his 2013 book of the same name dealing with terrorism in prisons.

[639] In this vein ECHR cases in which the internet interference was not proportionate under Article 10 include: Ahmet Yildirim v Turkey App.No.3111/10 (18.12.12) (indiscriminate blocking of access to Google); Cengiz and others v Turkey App.Nos.48226/10 and 14027/11 (1.12.15) (indiscriminate blocking of access to YouTube); Kharitonov v Russia App.No.10795/14 (23.6.00) (collateral effects of blocking IP address of shared web-hosting service).

peaceful majority and relieving tech platforms from the responsibility of moral arbitration.

11.29. However, it would be a mistake to conclude that terrorist content is simply too remote from violence. Experience shows that most terrorism arrestees are profoundly engaged in expressing and consuming violent and hateful material online, and that online encouragement can be troublingly effective at promoting violence in others, such as in the well-known case of RXG, a 14-year old British boy who incited an attack on the Anzac Parade in Melbourne, Australia [640].

11.30. The terrorist threat in Great Britain over the last decade has been dominated by Islamic State who propaganda proved effective at luring adults and teenagers to the so-called Caliphate. Islamic state would hardly put such store by publicly available content if online materials had no real world consequences: hence the observable concern of Islamic State when they are driven onto less publicly available channels[641].

11.31. There are patterns of mass ideological violence in the United States where the influence of online materials appears incontestable.

- The Buffalo (US) killer Payton Gendron was inspired by Christchurch (NZ) killer Brenton Tarrant who was inspired by the Norwegian terrorist Anders Breivik[642], and so on.
- According to a recent report by the New York Attorney General's Office, Gendron became radicalised on 4chan and Reddit where he became obsessed by white supremacy and the belief in white genocide. He plagiarized liberally from the Tarrant's manifesto, using up to 63% of Tarrant's text and in 23% of his own manifesto matching it word-for-word[643].

[640] RXG v Ministry of Justice and Persons Unknown [2019] EWCH 2026 (QB).
[641] Berger, J.M., Perez, H., 'The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters', occasional paper, GW Program on Extremism (2016)
[642] 'Buffalo shooting: How far-right killers are radicalised online', BBC News (17.5.22).
[643] Office of New York State Attorney General, 'Investigative Report on the role of online platforms in the tragic mass shooting in Buffalo on May 15, 2022' (18.10.22).

11.32. It would be irresponsible for the authorities in the UK not to be supremely mindful about similar violence in the UK, especially if effective 3-D printed guns took hold[644].

11.33. Broadly put, there is a mass of content online which has no terrorism impact on most viewers, but in respect of a small, perhaps infinitesimally small group of users, that content does translate into a material risk of terrorist violence.

- There is some sense in the government's modest assessment of the impact of the Online Safety Bill: although it is "…hard to quantify the benefit of the removal of terrorist content and activity from the online sphere", its removal will "…almost certainly have an effect on the level of terrorism in society" [645].
- However, how to define "terrorist content" is left wide open by this assessment, as is the question of whether certain forms of "terrorist content" are more likely to lead to violence than others.

Terrorist Offending

11.34. Further qualification is needed, drawing on the distinction between real world violence and terrorism offending.

11.35. Not all terrorism offences involve violence. The purpose of terrorism offences is to penalise conduct prior to an attack and enable the authorities to intervene early[646]. Encouraging terrorism or possessing terrorist manuals is criminal conduct but no one is necessarily harmed by it[647].

11.36. Because such offences are supremely easy to commit online, an online counter-terrorism policy must answer the following questions:

---

[644] Burgess, S, '3-D printed guns are appearing on British streets – and the police are taking notice' (Sky News, 15.6.22).
[645] HMG, Online Safety Bill Impact Assessment (31.1.22).
[646] In the matter of an application by Terence Marks for Judicial Review [2022] NIQB 57, at para 29, Scoffield J observed *obiter* that some criminal conduct such as membership of a proscribed organisation or weapons training could amount to 'terrorism' within the meaning of section 1, even though the use or threat of action was not an element of the offence charged. Nonetheless, even on this basis speech offences such as encouragement or dissemination could not amount to 'terrorism'.
[647] Under section 1(5)(a) Terrorism Act 2006, it is irrelevant whether or not a person is encouraged to carry out an act of terrorism.

- Is the justification for content removal the prevention of violence, or
- Is it sufficient justification that it may prevent the commission of terrorism offences?

11.37. An affirmative answer to the second question risks distortion to the 'harm principle' which ought to underpin counter-terrorism legislation: extraordinary measures may be justified but only if they reduce the risk of harm and not as ends in themselves[648].

11.38. The Online Safety Bill's use of the phrase "terrorism content" risks suggesting that content is inherently harmful by reference to a list of terrorism offences in Schedule 5 to the Bill; but content is not inherently harmful, what is harmful is terrorist violence, and its wider social effects, and the question is whether and to what extent restricting access to content makes terrorist violence less likely.

Counter-Radicalisation

11.39. Having examined some of the complexities that underly the identification of radicalising content, I turn to the rights and values that must be considered when formulating a response to online radicalisation. To be justified, counter-terrorism legislation (including the counter-terrorism aspects of the Online Safety Bill) must be effective in reducing the risk of terrorist violence but must also "…strike the right balance between the needs of security and the rights and liberties of the individual"[649].

11.40. What are the rights and liberties of individuals online? A complex picture emerges. At the end of this chapter, I draw a number of conclusions on how the value of freedom of expression can be sufficiently protected, whilst recognising that some content moderation is justified in the interest of preventing real world violence.

Rights

[648] See Lord Lloyd's second principle: "Additional statutory offences and powers may be justified, but only if they are necessary to meet the anticipated threat": Inquiry into Legislation against Terrorism (1996) at para 3.1.
[649] Inquiry into Legislation Against Terrorism, supra.

11.41. The first observation to make is that internet users do not enjoy fundamental rights in the traditional sense; and that the traditional mechanisms by which society considers (and if necessary, courts determine) whether a right ought to be qualified in the wider public interest is difficult to operate[650].

11.42. The purpose of making this observation is not to diminish the importance of holding online counter-terrorism to account, but to recognise that little light is shed by the pure assertion of rights in the online context. As one author has put it, appeals to fundamental rights online have come to resemble "policy advocacy clothed in the language of rights"[651].

11.43. Fundamental rights are invoked against states, either to forestall actions by the state against the individual (such as physical mistreatment), or to require them to put in place protection against harm from non-state actors[652]. But democratic states do not control the internet.

- In a case brought against Italy by a parents' association whose children had been targeted by obscene spam, the European Court of Human Rights agreed that the recipients' private life had been interfered with. However, the application was inadmissible because there was little that Italy could have done by way of counter measures[653].

11.44. On the contrary, life online is dictated by the capabilities of the platforms used, the commercial decisions those platforms make to allow, restrict or attract certain types of user, the speed of internet connection and the capacity of devices, and so on.

11.45. The second observation is that the internet is a networking of billions of individual users (and the tech companies themselves[654]) who in a rights-debate may appeal to standards that are materially different from the standards that underpin

[650] The proportionality exercise requires consideration of a 'fair balance' between individual rights and public interests: Bank Mellat v HM Treasury (No 2) [2013] UKSC 39 at para 20, Lord Sumption.
[651] Smith, G., 'Speech vs. Speech', (www.cyberleagle.com, 22 June 2021).
[652] As in KU v Finland App.No. 2872/02 (2.12.08) in which the ECtHR held that the government of Finland needed to have protective laws against online sexual abuse.
[653] Muscio v Italy App.No. 31358/03 (13.11.07).
[654] Cf. Case of Markt Intern Verlag GMBH and Klaus Beermann v Germany, App.No.10572/83 (20.11.89); Citizens United v Federal Election Committee, 558 U.S. 310 (2010).

fundamental rights as understood in the United Kingdom. Most significantly, the United States Constitution's First Amendment gives overriding primacy to freedom of expression even in cases where expression amounts to calls to violence and criminality[655], whilst section 230 of the US Communications Decency Act famously provides general immunity for service providers in respect of information provided by third parties[656].

11.46. Thirdly, even if individuals do enjoy rights, and the content of those rights can be agreed on, deciding on whether and how to enforce those rights is not straightforward:

- The internet has established social expectations[657] whose reversal is now inconceivable. Cutting off the internet, in the name of protecting the rights of potential terrorism victims, or indeed any measures that interfered with our demand for instantaneous information access and exchange, and faster and ever more efficient services, would not be tolerated in an open society[658].
- The public backlash against OnlyFans' decision to ban sexually explicit material on child safety grounds, forcing a reversal within 6 days[659], and consumer demand for the most secure levels of encryption despite the grave risk of consequence-free exploitation by terrorists and child sex abusers[660], illustrate the power of the market and however imperfectly, social expectations.

[655] Save in cases of "imminent lawless action": Brandenburg v Ohio, 395 U.S. 444 (1969). The position under UK common law and the ECHR is of course quite different because the right or freedom of expression may be proportionately curtailed in the wider public interest, specifically, in the terrorist context, in the interests of national security. Conversely, the UK (as a result of the ECHR) has adopted protections for privacy that go far beyond those applicable in the US. The position of the platform Gab is to enable any content that is protected by the First Amendment: Annual Report, 22 May 2020.

[656] The relationship between section 230 and immunity from suit for service providers allegedly involved in spreading terrorist propaganda is to be tested in the US Supreme Court in Gonzalez v Google 2021 USCA F3d and Taamneh, et al. v. Twitter, Inc., et al., No. 18-17192 (9th Cir).

[657] Cengiz and Others v Turkey, App.No. 48226/10 and 14027/11 (12.12.15) at paras 49 and 52. Of course, different societies have different social expectations: for example, the use of copyright protecting software is a major point of free speech contention in Poland (see Poland v European Parliament and Council of the European Union, Case C-401/19, 26 April 2022, Grand Chamber) but not, to date, the United Kingdom.

[658] For disabled users, the freedoms and opportunities created by the internet may be far more important than these advantages.

[659] Columbo, C., 'The history of OnlyFans: How the controversial platform found success and changed online sex work', Insider (14.9.21).

[660] Buhler, K., 'The Rising Consumer Demand for Data Privacy and Autonomy', Sequoia (18.11.21).

- Democratic states such as the United Kingdom have hitched themselves to powerful producer interests in accepting a free internet as vital for driving economic growth and providing innovative solutions[661].

11.47. Understanding the technical trade-offs between counter-terrorism and internet functionality is a closed book to those without detailed insider knowledge.

- Although the general need to balance innovation and global connectivity with counter-terrorism has been recognised by governments[662], it is difficult for the public or policy-makers to evaluate the argument that one or other regulatory burden would be a terminal threat to start-ups, or that content moderation is only possible through use of algorithms or machine learning that would have unintended consequences for internet use[663].
- There is a powerful case for greater transparency from tech companies to inform this debate[664].
- Governments are rightly wary of solidifying gains made by powerful producers – the Facebooks, Googles and Amazons – and recognise that a vibrant internet economy must embrace challengers. For example, the UK-based platform BitChute was established by 2 individuals in 2017 and by 2022 it had 12 employees and tens of millions of monthly visits[665]. Unfortunately, this free speech platform[666] quickly became a vehicle for Neo-Nazi propaganda[667]. Accommodating the business model of small platforms necessarily limits the extent to which regulation can be imposed.

11.48. A deep anxiety relates to those services on which the architecture of the internet depends (such as domain name providers) and concerns the desirability of imposing rules at this level for fear of politicising the internet leading to its eventual

[661] Declaration for the Future of the Internet (April 2022) to which the UK, US and EU Member States among others are signatories.
[662] Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes, New Delhi, India, 29 October 2022, at para 8.
[663] Gillespie, T., et al, 'Expanding the debate about content moderation: scholarly research agendas for the coming policy debates', Internet Policy Review Vol.9 Issue 4 (21 October 2020).
[664] Douek, E., supra.
[665] Bitchute, Transparency Report (June 2022).
[666] Trujillo, M, Gruppi, M., Buntain, C, Horne, B., 'What is BitChute? Characterizing the "Free Speech" Alternative to YouTube' (31st ACM Conference on Hypertext and Social Media, July 13–15, 2020).
[667] 'Hate Fuel: the online world fuelling far right terror', (CST, 1 May 2020).

fragmentation[668]. If the deep architecture of the internet is up for grabs, different countries will stake claims and seek to influence[669].

11.49. For example, the US company Cloudflare, which provides as much as 20% of the internet's protection against cyberattacks, has drawn a distinction between the types of services it provides based on their function[670] meaning that:

- Where the company provides hosting services (as the ultimate host of a website) it has a limited content restriction policy which the company says 'may' result in its removing content.
- For 'security services' (against cyberattack), Cloudfare will no longer impose any of its own restrictions. Famously, Cloudfare removed security services for the neo-Nazi site 'the Daily Stormer' in 2017, and the notorious forum '8Chan' in 2019, leaving them open to cyberattack. It now says it will never do this again, on the basis that cyberattacks 'should be relegated to the dustbin of history', and only comply with legal obligations arising in the US where it is headquartered[671].
- For 'Core internet technology services' such as DNS services, Cloudfare says that it is providing global services and will seek to resist attempts to impose any restrictions whatsoever.

11.50. Finally, the vibrancy of the online market for platforms and apps means that restrictions on content on one platform are unlikely to be decisive for rights. The internet is not a single geographical entity where forbidding free expression would be terminal. If, say, TikTok decided to bar political activity, the damage to rights could be mitigated or avoided by migrating to Twitter. Heavy restrictions on content on platforms aimed at children have no impact on the rights of adults.

11.51. At the very least, the task of identifying how the public interest interacts with the enjoyment of individual rights is extraordinarily complex.

---

[668] Bennett, A., Garson, M., Boakye, B., Beverton-Palmer, M., Erzse, A., 'The Open Internet on the Brink: A Model to Save Its Future' (Tony Blair Institute for Global Change, 2021).
[669] Hence the caution expressed by Tech Against Terrorism, Strategy Paper 'Responding to Terrorist Operated Websites' (July 2022) at page 6.
[670] Cloudflare Blog, 'Cloudflare's abuse policies and approach' (31.8.22), https://blog.cloudflare.com/cloudflares-abuse-policies-and-approach/, last accessed 1.9.22.
[671] However, shortly after this policy was announced, Cloudfare did block a website strongly linked to violence: CloudfareBlog, 'Blocking Kiwifarms' (3.9.22).

11.52. Finally, if it is correct that fundamental rights suggest the existence of procedural protections[672], realism is required about what this might mean in practice[673].

- It might be said that to protect the right of free expression, no content should ever be removed without a court order or at the very least some form of independent adjudication[674],
- However, because of the scale of content that may need to be processed, the intervention of a human moderator, subject to judicial review before an independent tribunal, cannot possibly be guaranteed for every takedown decision made by a platform – even disregarding the jurisdictional difficulties of identifying a moderator and judge who could authoritatively decide on content posted anywhere in the world.

Values

11.53. Because of these difficulties, and although the language of rights continues to be widely used in the online context[675], it is somewhat easier to refer to consider rights as values.

11.54. One potential benefit to this approach may be to temper the assertiveness that sometimes comes with discussion of rights. That can only be beneficial pending greater understanding of the costs and consequences of online speech. Consideration of whether and when the right to freedom of online expression is

[672] As Hickman, T., 'Public Law after the Human Rights Act' (Hart, 2010) at p226 et seq, discusses, the question of whether individual rights imply separate procedural protections is not straightforward.
[673] Douek, E., Content Moderation as Administration (January 10, 2022). forthcoming Harvard Law Review Vol. 136
[674] As suggested by Smith, G., 'Should We Be Building Online Prior Restraint Machines' (Society for Computers and Law, 22.1.18).
[675] For example, Tech Against Terrorism "…aim is to counter terrorist use of the internet whilst respecting human rights" (TCAP Transparency Report (March 2022) at para 4.2.1.). But this cannot refer a duty on the part of Tech Against Terrorism to protect the human rights of unspecified rights-holders. It is more coherent to understand this mission statement as a commitment to encouraging governments and tech companies to recognise certain values in the decisions they make. Similarly, although the second iteration of the Santa Clara Principles was designed to "support companies to comply with their responsibilities to respect human rights", it is telling that the principles themselves refer to "human rights *considerations*" (Foundational Principles, para 1) (my emphasis) - a tacit recognition that human rights in the reciprocal-duty sense do not apply.

trumped by rights to life and bodily integrity in the real world requires some humility in appreciating the complex interaction between the online and offline worlds.

11.55. These uncertainties place especial value on the sincere implementation of transparency, the second of the so-called 'Santa Clara Principles' [676]. The development of principled counter-terrorism strategies is best done through open debate and exposure of rules and policies, not hole-in-a-corner decisions that come to light late if at all. I refer to transparency not simply for the terms and conditions deployed by tech companies, or laws and practices developed by countries[677], but of the trade-offs that lie behind public positions.

- I refer in Chapter 12 to the difficulties in identifying why tech companies make the rules that they do, or how effectively they will enforce the standards they purport to hold: there is no guarantee that tech companies will be honest about the cost consequences for them if, for example, they tweak an algorithm or introduce a new set of community standards.

11.56. The key rights or values against which counter-online radicalisation efforts must be judged are those of freedom of expression and privacy/correspondence, although not without reference to the (under-developed) values of protecting children in the online space.

11.57. Freedom of expression encompasses the ability to impart and receive information and, as well as being inherently valuable, is considered to protect three values: those of truth, democracy and individual autonomy or self-fulfilment[678]. It has long been formulated in terms of receiving and imparting information "regardless of frontiers"[679]. It is unsurprising then that the UN General Assembly Resolution, adopted at the 65th plenary meeting, 14 December 1946, emphasised that 'Freedom of information is a fundamental human right and is the touchstone of all freedoms to which the United Nations is consecrated'.

[676] https://santaclaraprinciples.org.
[677] As in *Malone v UK*, App no 8691/79, (1984) 7 EHRR 14.
[678] These three values identified in Frederich Shauer, 'Free Speech: A Philosophical Enquiry' (Cambridge, 1982) were deployed by Lord Steyn in R v Secretary of State for the Home Department, *ex parte Simms* [2000] 2 AC 115 at 126.
[679] Article 19 Universal Declaration of Human Rights; Article 19 International Covenant on Civil and Political Rights; Article 10 ECHR.

11.58. The first of the three values, truth, is particularly resonant in the terrorism context. Terrorist attacks change nations. Activities of violent diaspora groups linked to overseas conflicts, or violent domestic movements, are part of world history and personal experiences. The terrorist/ freedom fighter dilemma is inescapable, and content posted for sinister reasons may nonetheless be a true record. Where content, however disturbing, is used to tell the truth about an individual's own experience, the law rightly regards the ability to do this as a "basic right" to which the law gives "a very high level of protection"[680]: in less legalistic terms, truth is "our richest merchandise"[681].

11.59. Since terrorist groups (such as Da'esh/ Islamic State) are principal actors in world-changing events, there is truth value in knowing or establishing the truth about groups or individuals pursuing social change through violence[682] and holding them accountable. Automatic content removal may have the effect of airbrushing the historical record[683] whereas images from conflict zones may be important sources of evidence that can be used in legal proceedings[684].

11.60. This places a value on access to disturbing footage and blatant propaganda – and not merely for academics or journalists.

- Its value to the historical record may not be obvious at the time.
- The purpose for which the information was posted online does exclude its utility in establishing the truth.
- The value of compiling a truthful record provides a strong imperative to allow content to be posted and once posted to secure it, so that all internet content is kept for future reference and not destroyed.

11.61. Whilst online content is not notorious for its adherence to truth, even demonstrably false content will generate true metadata: a time and date, technical information, and potentially clues as to the identity of the person who posted the

[680] James Rhodes (Appellant) v OPO (by his litigation friend BHM) and another (Respondents) [2015] UKSC 32 at para 76, 77.
[681] Milton, J., 'Areopagitica' (1664).
[682] Which is why, as Professor Maura Conway points out, removing only violent propaganda made by terrorist organisations and leaving up the happy material (pictures of nurseries etc.) distorts the truth about the nature of these organisations.
[683] An example regarding Syrian atrocities is given by MacDonald, S., Correia, S., Watkin, A., supra.
[684] As in the prosecution – in the US – of the so-called 'Beatles' formerly led by Mohammed Emwazi ('Jihadi John').

falsehood. Truth may also be expressed in different guises (by novels or songs[685], such as nasheeds or anashids**,** a subset of which celebrates jihadi violence and are produced by IS/Da'esh[686]) and freedom of expression protects choice as to how to express truth[687] including offensively[688]. Content exposes how individuals were using the internet at that point in time: referred to as the 'use meaning' rather than the 'representational meaning' of the words, images and sounds encountered[689].

11.62. This is consistent with the position taken by search engines such as Google to index, and ultimately make available to the general user, all surface web content[690]. On this basis search engines should be as neutral as possible, leaving responsibility for removing radicalising content to others, despite the gateway role played by search engines for those who are broadly interested to discover content that confirms the acceptability of violence.

11.63. It follows that there is at least some value in protecting content even if the motives of the content provider are so abusive that they themselves may be said to have forfeited reliance on a fundamental right[691].

11.64. The mission of sites such as the Internet Archive (archive.org) is not just to preserve but to maintain general availability: "Universal access to All Knowledge"[692]. Europol assessed that jihadi propogandists were exploiting the Internet Archive for their own purposes[693] by making use of its permanency and openness.

---

[685] Article 10 ECHR applied as much to the songs of Pussy Riot as to the symbolic display of dirty laundry near the Hungarian Parliament: *Mariya Alekhina and Others v Russia* (2019) 68 EHRR 14.
[686] Velasco-Pufleau, L., 'Jihadi Anashid, Islamic State Warfare and the Agency of Sound', Crime and Music, Springer, pp.233-243, 2021.
[687] Per Lord Neuberger in Rhodes, supra, citing Campbell v MGN Ltd [2004] UKHL 22, [2004] 2 AC 457, para 59, and In re Guardian News and Media Ltd [2010] UKSC 1, [2010] 2 AC 697, para 63.
[688] Sedley LJ in *Redmond-Bate v Director of Public Prosecutions* (1999) 7 BHRC 375, [20].
[689] Blocher, J., 'Nonsense and the Freedom of Speech: What Meaning Means for the First Amendment', [2014] Duke Law Journal vol.63: 1423.
[690] Google, 'Maximise access to information' https://www.google.com/search/howsearchworks/mission/open-web/ accessed 13.5.22).
[691] The ECtHR held in *Norwood v United Kingdom* App No 23131/03 at para 4 that a poster advocating the removal of Islam from the UK because of the 9/11 attacks did not enjoy the protection of Article 10 in light of Article 17 (abuse of rights). The invocation of Article 17 in this context looks like an overreaction and is not without its critics: A Buyse, "Dangerous Expressions: The ECHR, Violence and Free Speech" (2014) 63(2) *International & Comparative Law Quarterly 491*. The better explanation may well be that Mr Norwood's conviction for incitement to hatred and violence was justifiable because his freedom of expression was acceptably qualified in the wider public interest.
[692] "About the Internet Archive" (archive.org/about/, accessed 11 May 2022).
[693] Europol, 'Jihadist content targeted on Internet Archive platform' (press release, 16 July 2021).

11.65. Next, the ability of individuals to participate in public decision-making, and therefore democracy, is nothing without freedom of speech: the free flow of information and ideas informs political debate and voting, is a safety valve because people are more willing to accept adverse decisions if they can seek to influence them through, and acts as a brake on the abuse of power by public officials and others[694].

11.66. The internet is one of, if not the principal means[695] by which individuals find information relevant to public life, whether through traditional newspapers and broadcasters that have gravitated online, or through untrained members of the public operating as citizen journalists such as *The Sandwell Skidder*[696] or simply users of social media[697].

11.67. Images from conflict areas in which terrorists are active, including of the terrorist acts of the so-called Islamic State Beatles in Syria, are important documents in informing democratic debate on vital matters of public policy. Sometimes editorial judgment may call for the use of shocking images including what might be described as terrorist propaganda.

11.68. The third interest instrumentally protected by freedom of expression is individual autonomy or self-fulfilment. Arguably, this is the dominant mode of use: private trivial or homely communications which serve no purpose other than tending to interpersonal relationships.

- For some people, online engagement will be vital to the promotion of these interests: for example, video-conferencing by someone confined to bed, or membership of an online support group for sufferers from an extremely rare disease. Freedom of expression underpins freedom to associate[698] to which digital technology and online spaces are now integral[699].

---

[694] Lord Steyn, ex parte Simms, supra; *R v Shayler* [2003] 1 AC 247, [21]. In an era of disinformation it would be naïve not to recognise that the internet calls into question JS Mill's characterisation of the free competition of ideas as the best way to separate falsehoods from fact.
[695] Cf. Mustafa v Sweden, 16.12.08 in which the internet was the only means of hearing news in the applicant's home language.
[696] McNally v Saunders [2021] EWHC 2012 (QB), with thanks to Graham Smith for this reference.
[697] *Magyar Helsinki Bizottság v Hungary* (2020) 71 EHRR 2 at para 168.
[698] Article 20 Universal Declaration of Human Rights; Articles 21 and 22 International Covenant on Civil and Political Rights; Article 11 ECHR.
[699] UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Report to Human Rights Council (17 May 2019).

- It is true that much online engagement is objectively deleterious to personal development. Individuals do not bring their 'best selves' to the internet, as David Baddiel has memorably illustrated[700]. The combination of wanting a tribe, vying for shock value, and the freedom from convention that comes with (generally) anonymous engagement means that online personalities may be considerably more sympathetic to terrorist violence than their owners are away from the screen – indeed different personalities all together[701].
- But, despite the occasional desire of autocratic governments and frustrated parents to pull the plug on the internet, it is now too central to the way we all communicate and find meaning to wish it away.

11.69. Privacy[702] protects expression of individuality and an inner life, the facilitation of trust, friendship, and intimacy (particularly for people with disabilities or social communications problems[703]), the securing of other rights (for example by protecting journalistic sources), and empowering individuals against the state[704]. These interests will be in play when a lonely individual, perhaps an autistic adolescent with no friends at school finds purpose and solace through membership of an online group of Second World War enthusiasts: the problem comes when members of the group start to fixate on Nazi memorabilia, then violence against Jews and Muslims.

11.70. These values are relevant to children as much as to adults[705]. However, the adverse impact on children of society's great internet experiment is less coherently recognised in international instruments.

- In the main, harm from the internet is seen as relevant under existing thematic categories such as sexual exploitation[706].
- The European Commission's "framework to protect children's rights in the digital environment" is a collection of miscellaneous instruments, presented

[700] David Baddiel: Social Media, Anger and Us (BBC 2, 14 December 2021).
[701] Blumer, T., Döring, N., "Are we the same online? The expression of the five factor personality traits on the computer and the Internet", Cybersecurity 6(3) (December 2012).
[702] Article 12 Universal Declaration of Human Rights; Article 17 International Covenant on Civil and Political Rights; Article 8 ECHR.
[703] Re: A (Capacity: Social Media and Internet Use: Best Interests) [2019] EWCOP 2, Cobb J., at para 2.
[704] Anderson, D., 'A Question of Trust: Report of the Investigatory Powers Review' (June 2015) at paras 2.10 to 2.13.
[705] UN Convention on the Rights of the Child, arts. 14 to 16.
[706] E.g. UNICEF, 'Protecting children online': https://www.unicef.org/protection/violence-against-children-online (last accessed 24.10.22).

under the dubious introduction "…Children are digital natives"[707] which implies a cheery sense that children are less at risk than adults.

11.71. The Council of Europe has proposed Guidelines (2018) that include the proposition that, "Taking into account the development of new technologies, children have the right to be protected from all forms of violence, exploitation and abuse in the digital environment" and refer to the risk of harm from online recruitment for participation in extremist movements[708]. There is reference to the need for precautionary measures given the speed that emerging technologies can impact on children[709].

11.72. In 2021, the UN Committee on the Rights of the Child promulgated a general comment on children online[710]:

- It refers to risks relating to content, contact and conduct relating to the promotion of "life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist."[711]
- It calls on State parties to protect children from harmful content "in accordance with their rights and evolving capacities"[712].
- It recognises that the digital environment can open up new ways for terrorist groups to recruit and exploit children to engage with or participate in violence[713].

11.73. However, this document contains only oblique recognition ('evolving capabilities') of the special susceptibility of children to the content they encounter online[714]. As will be apparent from this report, it does appear that children are particularly susceptible to terrorism content and being drawn into terrorism offending,

[707] 'Digital and Information Society: Thematic area 5 of the EU strategy on the Rights of the Child': https://ec.europa.eu/info/policies/justice-and-fundamental-rights/rights-child/digital-and-information-society_en (last accessed 24.10.22).
[708] 'Guidelines to respect, protect and fulfil the rights of the child in the digital environment' at para 50.
[709] Ibid, para 52.
[710] UN Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment'.
[711] Para 14.
[712] Para 54.
[713] Para 83.
[714] Para 19-21.

although it is an open question whether this means that they will go on to commit acts of violence.

Conclusions

11.74. Firstly, the aim of content removal in the name of counter-terrorism must be to reduce terrorist violence not merely terrorist offending.

11.75. Secondly, the question of whether content may radicalise to violence should be evidence-based.

11.76. Thirdly, it is neither possible nor justifiable to remove all potentially radicalising content.

11.77. Fourthly, if (by contrast) terrorist offending is to be used as a metric, the special susceptibility of children must be considered.

11.78. Fifthly, even in cases of clearly radicalising material, the impact of content removal needs to be mitigated by allowing editorial judgments by responsible media, access by bona fide researchers, and availability for investigation and prosecution[715].

11.79. Sixthly, because the trade-offs are difficult to understand, there must be transparency in how material is selected for moderation.

[715] As permitted by New Zealand's Films, Videos, and Publications Classifications Act 1993, section 44, in respect of banned materials.

12. **CONTENT MODERATION**

12.1. In this chapter I have endeavoured to describe the roles played by tech companies and their membership organisations in counter-terrorism, principally by means of content moderation. I then consider the adequacy of UK legislation.

Tech Companies

Generally

12.2. There are two reasons why the implementation of online counter-terrorism must be for tech companies, at least in free societies:

- Firstly, governments have neither desire nor the capacity to dictate how tech companies operate. Authorities find it difficult to keep pace with evolving platforms and technological change[716].
- Secondly, the sheer volume of online content means that effective moderation is inevitably machine-led[717], and the machines and the systems within which those machines operate belong to tech companies not governments. It has been reported that in 2020, more than 500 hours of video was uploaded to YouTube every minute[718].

12.3. This is not to say that democratic governments have no role in influencing what should be implemented; and tech companies have increasingly asked greater guidance, for example by designating, and assisting with the attribution of websites to, terrorist organisations[719].

[716] MacDonald, S., Staniforth, A., 'The Tech Industry and the Regulation of Online Terrorist Content: What do Law Enforcement Think?' (Hedayah Center) quote a law enforcement official "The technology is outpacing how we think about managing these risks and issues'. An example is decentralised Blockchain technology.
[717] McDonald, S., Correia, S., Watkin, A., 'Regulating terrorist content on social media: automation and the rule of law', International Journal of Law in Context, 15(2), 183-197.
[718] https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/ (last accessed 1.9.22).
[719] Reflected in Tech against Terrorism, 'The Online Regulation Series' (July 2021).

12.4. Total outsourcing of counter-terrorism to private companies could lead to a loss of trust in civil society and in government[720], alongside with legitimate fears that tech companies are ill-equipped to make decisions touching on terrorism and national security[721].

12.5. On the other hand:

- It may be convenient for tech companies to try and shift responsibility for their own inaction by pointing to lack of government guidance or intervention.
- The more tech companies are seen to cooperate with governments, the less confidence users may have in the integrity of the platform, leading to an exodus towards the least cooperative[722].

12.6. In its 2018 national security strategy document, Contest 3.0, the government referred to its intended relationship between the government and private tech companies as a partnership [723]. Until recently, this partnership involved the government cajoling companies, marshalling opinion, convening meetings, and flagging content, based on a recognition that tech companies could not be forced to act.

- This 'soft law' has been criticized on the basis that it is harder to detect whether human rights standards are being upheld[724].

12.7. The trend now is that governments should have a role in *determining* the counter-terrorism measures that tech companies should implement. The Online Safety Bill identifies these measures at a macro-level in the form of duties of care; the EU Digital Services Act allows national authorities to dictate to tech companies at a

[720] Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Human rights impact of policies and practices aimed at preventing and countering violent extremism' (2020), at para 22.
[721] Tech Against Terrorism, 'The Online Regulation Series: The Handbook', at page 19.
[722] David, G., 'Bitchute: Platforming Hate and Terror in the UK', Hope Not Hate. Since then Bitchute appears to have changed its approach - it joined the membership organisation Tech Against Terrorism in 2022.
[723] At para 80.
[724] Ní Aoláin, F., 'Soft Law', Informal Lawmaking and 'New Institutions' in the Global Counter-Terrorism Architecture (2021) 32 *European Journal of International Law* 919. Clifford, B., supra, contains a useful discussion of the relationship between hard and soft laws; cf her letter to Mark Zuckerberg on the definition of terrorism (24.7.18, Ref: OL OTH 46/2018).

micro-level, by requiring the removal of individual items of content. Tech companies risk facing an increasing number of different regulatory environments[725].

12.8. Content moderation is the go-to remedy for online radicalisation because it is seen as removing the problem at source. Since no content is automatically radicalising and it is impossible to remove all content that might in fact radicalise[726], it would be more accurate to say that content take-down is in principle capable of reducing the risk of terrorist violence.

12.9. It is however true to say that removing content in this way means it cannot be downloaded by anyone; an alternative, proposed by Apple as a means of dealing with encrypted child sex abuse imagery, but then withdrawn in the face of market pressure, is client-side scanning[727].

12.10. The scale and complexity of the internet means that content removal is not a once-and-for all process. Islamic State propaganda has proven hydra-headed, jumping between platforms, and reappearing on lesser sites, in response to law enforcement[728]. Content moderation may be about achieving a tactical win but never a final victory.

12.11. There are other methods of online counter-terrorism. Major tech companies (at least) have the capacity to:

- Implement age barriers, geo-blocking, or temporary holds, to keep content away from some users some of the time.
- Add fact-checking labels and warnings, to alert users to content before or as they encounter it.
- Impose disincentives for producing content, such as demonetization and punitive strike system.

[725] GIFCT has a useful interactive graphic: https://gifct.org/global-legislative-map/#/map (last accessed 17.10.22).
[726] See Chapter 11.
[727] 'Apple quietly deletes details of derided CSAM scanning tech from its Child Safety page without explanation' (The Register, 16.12.21).
[728] Lakomy, M., GNET Insights (17.5.22); Tamar Mitts, Countering Violent Extremism and Radical Rhetoric (2021) 76 *International Organizations* 251.

- Reduce the visibility or reach of content by tweaking recommendation systems, or in increasing download speeds or introducing glitches to certain content[729].
- Add friction by, for example, making it more difficult to re-post at scale[730].

12.12. For infrastructure companies, removing services from an entire platform may be a response to terrorist material on that platform: for example, Bid Glass terminated its services for 4chan after the Buffalo attack, Cloudfare removed its content deliver network service from 8chan after various mass shootings, and Voxility and Bitmitigate withdrew services from Epik[731].

12.13. The counterpoint to reducing interaction with radicalising content is the search for online de-radicalisation. One potential method is to provide context about the content displayed to reduce its radicalising force[732] or redirect users to benign sites[733].

- However, success may be difficult to verify not least because of the difficulty of intelligence sharing between the intelligence world and researchers[734] and between platforms, so that a proper understanding can be gained of whether the user has lot their taste for terrorism-promoting content.

- My own observation, drawn from over three years' attendance at meetings of the TPIM review group[735], is that theological or ideological interventions in real life cannot be counted on, other than at a level of providing human support to isolated individuals. There is no particular reason to believe that ideological persuasion is any more likely to operate effectively online.

Attitudes and Capability

[729] Gillespie, T., 'Do Not Recommend? Reduction as a Form of Content Moderation', Social Media + Society July-September 2022: 1–13.
[730] As advocated by the Facebook whistle-blower, Frances Haugen: see for example, oral evidence to Joint Committee on the Online Safety Bill (25 October 2021).
[731] Office of New York State Attorney General, 'Investigative Report on the role of online platforms in the tragic mass shooting in Buffalo on May 15, 2022' (18.10.22).
[732] Referred to as "counter-speech": see for example, Saltman, E., Kooti, F., Vockery, K., New Models for Deploying Counterspeech: Measuring Behavioral Change and Sentiment Analysis, (2022) Studies in Conflict & Terrorism.
[733] In 2019, Facebook and Instragram announced that they would divert people who search for terms associated with white supremacy to a counter-extremism group: Meta, 'Standing Against Hate' (27.3.19).
[734] Marc Sageman (2014) The Stagnation in Terrorism Research, Terrorism and Political Violence, 26:4.
[735] Terrorism Acts in 2018 at 8.18 et seq.

12.14. The tech-utopian dream of universal knowledge and communications freed from the deadening regulation and attention of worldly states, coupled to a recklessly indifferent dash for growth, led to a certain reluctance on the part of tech companies to control terrorism content.

12.15. Tech companies are and have always been more proactive against child sex abuse material (CSAM), and have mostly been willing to accept the compliance costs that come with it. The same is true of responding to allegations of copyright infringement. Terrorism was not in the same category, and the unleashing of Islamic State propaganda on tech platforms in the mid-2010s evoked, were the potential consequences not so serious, the position of football clubs unwilling to pay for crowd control.

12.16. According to Facebook's former head of CT, the tech community was regrettably slow in taking counter-terrorism efforts seriously[736].

12.17. Other reasons for collective delay were more forgivable: engaged companies found it hard to create universal rules for terrorism content across multiple jurisdictions in the absence of an internationally agreed definition of terrorism, and where the designation by one state of individuals or groups as terrorists could be highly contested in another.

12.18. A series of factors led to greater proactivity in the second part of the 2010s:

- The rise of Islamist State and its use of online propaganda[737].
- Pressure from governments, and the threat of regulation.
- Market pressure[738] and bad publicity.

[736] Fishman, B., 'Crossroads: Counter-terrorism and the Internet', Texas National Security Review (2019) Vol 2, Iss 2.
[737] Clifford, B., 'Moderating Extremism: The State Of Online Terrorist Content Removal Policy In The United States', George Washington University Program on Extremism (Dec 2021).
[738] Including pressure from suppliers of security and cloud hosting services: see e.g. 'Two more platforms have suspended Gab in the wake of Pittsburgh shooting' (The Verge, 28.10.18).

- Greater internal acceptance of responsibility following attacks such Christchurch New Zealand in 2019 where the internet appears to have played an important role[739].

12.19. A further factor in future may be legal pressure in the US[740].

12.20. The result is that the larger (and some smaller) platforms have moved significantly towards accepting (some) responsibility for removing (some) terrorist content. However, whilst large platforms have thousands of employees, including teams of counter-terrorism specialists (frequently recruited from government or law enforcement) who may be personally enthusiastic, willingness to act is bounded by commercial interests and subject to the views of powerful founding owners[741].

12.21. Tech companies and their attitude to counter-terrorism have been categorised as follows[742]: (i) those lacking awareness and expertise; (ii) those lacking capacity and resources; (iii) those lacking willingness; and (iv) those who have awareness, expertise, capacity, resources and willingness.

12.22. An example of differential willingness is found in the response to content flagging by government or third parties. Tech Against Terrorism found that archiving platforms were least responsive to their alerts of terrorism content[743]. Some tech companies such as Gab position themselves as champions of free speech with a default position against restraining content[744].

---

[739] Clifford, B., 'Moderating Extremism: the State of Online Terrorist Content Removal Policy in the United States', George Washington University (December 2021).
[740] Social media companies have been sued in the US for allowing terrorism uses. The claim in Fields v. Twitter, 217 F. Supp. 3d 1116, 1118 (N.D. Cal. 2016), affd, 881 F.3d 739 (9th Cir. 2018) failed by reference to causation or the Communications Decency Act 1996, section 230 immunity. In Goldstein v Facebook USDC 12 August 2020 the claimant unsuccessfully sued Facebook for aiding international terrorism by helping attacks in Kenya and Sri Lanka. However, the claims in Gonzalez v Google 2021 USCA F3d (damages under 18 USC s.2333 for attacks by ISIS in Paris, Istanbul and San Bernadino, on the basis of Google's enjoyment of advertising revenue) and Taamneh, et al. v. Twitter, Inc., et al., No. 18-17192 (9th Cir.) a claim brough by relatives of a victim of the 2017 Istanbul night club attack. The US Supreme Court has agreed to hear appeals on both these cases.
[741] For example, Facebook's decision to ban holocaust denial was based on Mark Zuckerberg's own change of heart: 'Facebook banks Holocaust denial content' (BBC News, 12.10.20).
[742] Watkin, A. (2021) 'Regulating terrorist content on tech platforms: A proposed framework based on social regulation.' PhD Thesis. Swansea University.
[743] TCAP Report, 'Terrorist Content Analytics Platform: Year One: 1 December 202 to 30 November 2021', at page 3.
[744] Gab terms of service: https://gab.com/about/tos (last accessed, 13.10.22).

- There may also be distinctions relating to the type of content. Tech against Terrorism found that the average removal rate by tech companies following alerts of Islamist terrorist content was 94%, whereas the average removal rate of far-right terrorist content was 50%[745].

12.23. Larger tech companies operate notification systems for 'trusted flaggers', who have a more direct route to notify tech companies about terrorism content found on their platforms. But even law enforcement find that this route is heavily dictated by companies; I was surprised to learn that CT Police are not given contact phone numbers by certain platforms. Even large companies draw the line at making referrals of terrorist material to law enforcement (other than in cases of threat to life).

12.24. Capacity is a major factor for all companies given the global reach of the internet. For Meta, "…some regions may have more in-country personnel, language and translation services, moderation capacity, or technical interventions than others"[746]. Companies will often lack the capacity to read even major languages: for example, an inability to scan Sinhalese allowed major platforms to be used for anti-Muslim violence in Sri Lanka[747], and a lack of skill in local languages affects content moderation in Afghanistan[748].

12.25. The margins for smaller companies will often be very small. They may lack the revenue streams to employ someone for content moderation[749]. Terrorist groups can suddenly exploit a new online tool, as Islamic State/Da'esh did with one-man-band JustPaste.it[750]. The price of innovation and an open internet is that starter-companies will simply lack removal architecture; and if they do not agree with content moderation in principle they will never invest in moderators.

12.26. Tech companies are not investigators with an ability to probe the human intentions behind a particular post. Determining whether something falls the wrong side of the line is often an evaluative exercise and may depend on legal specialism in

[745] TCAP Report, supra, at page 3.
[746] BSR, 'Human Rights Impact Assessment: Meta's Expansion of End-to-End Encryption' (2022).
[747] Where Countries Are Tinderboxes and Facebook is a Match', New York Times (21.4.18). See also Chapter 1 at REF.
[748] Scott, M., 'Facebook did little to moderate posts in the world's most violence countries' (Politico, 25.10.21).
[749] MacDonald, S., Staniforth, A., supra.
[750] 'How a Polish student's website became an ISIS propaganda tool' (Guardian, 15.8.14).

counter-terrorism (which all companies and membership organisations lack). Sometimes that exercise will be inescapable for tech companies operating in jurisdictions where their activity might expose their own employees to criminal liability.

Role of Terms and Conditions in Counter-Terrorism

12.27. Tech companies based largely abroad have no reason to base their contractual relationship with users on the Terrorism Acts 2000 and 2006. In the absence of a universal definition of terrorism[751], relevant terms and conditions tend to be those which relate to violence or its encouragement[752], dangerousness, or hate between groups. Terms that prohibit this type of conduct ought, if implemented, to capture most terrorist content.

12.28. What terms and conditions do provide is authority for tech companies to remove content when it is found to be in breach. A survey of law enforcement personnel whose role was to draw terrorist material to the attention of tech companies found that officials rarely referred to violation of national laws: they focussed instead on the fact that content breached the company's terms of service[753].

12.29. But the role of Ts and Cs should not be overstated:

- Anyone who wishes to find harmful or dangerous content on a platform can usually find it, even though entirely at odds with the company's published standards. Prohibitions on violent content do not equate to an absence of violent content if the company is not aware of it or lacks the willingness or ability to enforce standards.
- Tech companies' most effective contribution to counter-terrorism comes by way of automation (discussed below).
- How tech companies promote or limit content may be the product of policies which are obscurely introduced[754].

[751] Facebook had a well-resourced shot at achieving a workable definition. Their evolving community standards reflect the arguments that make finding a universal definition so difficult.
[752] For example, Meta's 'Violence and incitement' policy: https://transparency.fb.com/en-gb/policies/community-standards/violence-incitement/ (last accessed 13.10.22).
[753] MacDonald, S., Staniforth, A., blog, supra.
[754] Gillespie, T., 'Do Not Recommend? Reduction as a Form of Content Moderation', Social Media + Society July-September 2022: 1–13 reveals how forms of moderation were are quietly introduced by Facebook in a run of posts.

- Terms and conditions may be subject to unpublished exceptions (an interesting example concerns the Taleban after the 2021 withdrawal of US and UK troops[755]) or published exceptions (such as YouTube's exceptions for 'Educational, Documentary, Scientific or Artistic' content[756]).

12.30. Nor should the difficulty of producing a comprehensive but sufficiently nuanced set of terms and conditions be underestimated.

- Crafting terms that prohibits both official publications by terrorist groups and unofficial propaganda that praises them, needs to cater for support for a group's non-violent activities.
- Whilst it might easily be said that any support of any of Islamic State's activities should be prohibited, it is more difficult to say this of content supporting positive steps by terrorist groups who exercise political control in Afghanistan or the Occupied Territories.
- To ban such content could restrict political discussions in some locations.
- This is before one even needs to consider exceptions for journalism or documenting human rights abuses[757].

Examples of terrorism-related Terms and Conditions[758]

12.31. Meta has highly developed Community Standards[759]. The rational for their 'Dangerous individuals and organisations' policy is "to prevent and disrupt real-world harm", and groups and individuals are grouped into 3 Tiers.

- Tier 1 includes "terrorist, hate and criminal organisations" *including* (but not apparently limited to) those designated by the US government. Tier 2 are "violent non-state actors" who engage in violence against state or military

[755] 'Facebook bans Taleban but Twitter adopts more 'laissez fair' approach' (Euractiv, 24.8.21); 'Facebook Grants Government of Afghanistan Limited Posting Rights' (the Intercept, 23.11.21). These articles state that Twitter and Facebook introduced unpublished exceptions for the Taleban or certain members of the Taleban.

[756] https://blog.youtube/inside-youtube/look-how-we-treat-educational-documentary-scientific-and-artistic-content-youtube/ (last accessed 14.10.22).

[757] Cf. the interesting discussion in Fishman, supra.

[758] Allowance should be made for the updating of terms and conditions, and I include within this category 'Community Standards' and published policies.

[759] https://transparency.fb.com/en-gb/policies/community-standards/dangerous-individuals-organizations/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fdangerous_individuals_organizations (last accessed 13.10.22).

actors. Tier 3 concerns entities that have not yet committed violence or directly called for violence, but are on the cusp (e.g. "violence-inducing conspiracy networks").

- Content relating to individuals and groups in different tiers in principle gets slightly different treatment (for example, banning praise of their founders, or not).
- In addition to individuals and groups, Facebook designates "violating violent events" and their perpetrators. There is no published list, but one can assume that this is intended to prevent, for example, praise of Brenton Tarrant's attacks at Christchurch New Zealand.
- The policy is also to remove content that praises or supports "ideologies that promote hate, such as Nazism and white supremacy". Illustrating the point that terms and conditions are not a guide to platform content, after typing the last sentence I immediately found content on Facebook praising the neo-Nazi James Mason and his deeply influential book 'Siege'.

12.32. According to Meta's figures, in the last three months of 2021 Facebook actions 7.7 million pieces of content based on its 'Dangerous individuals and organisations policy'[760].

12.33. In the moderately developed category:

- TikTok has a 'Violent extremism' policy which bans "terrorist organisations" (not defined by reference to designation), organised hate groups and criminal organisations from their platform, and forbids the promotion etc of violence[761].

- Google-owned YouTube's 'Violent criminal organizations policy' is tied to content produced by terrorist organisations or content praising terrorists or terrorist organisations or their actions[762]. Terrorist activity that is not linked to

[760] Meta, Management Report on community standards enforcement for the period 1.10.21 to 31.12.21: https://about.fb.com/wp-content/uploads/2022/05/EY-CSER-Independent-Assessment-Q4-2021.pdf (last accessed 13.10.22).
[761] https://www.tiktok.com/community-guidelines?lang=en#39 (last accessed 13.10.22). Since March 2021 its content moderation policies and practices are said to be subject to advice from its "European Safety Advisory Council': https://newsroom.tiktok.com/en-gb/tiktok-european-safety-advisory-council (last accessed 14.10.22).
[762] https://support.google.com/youtube/answer/9229472?hl=en&ref_topic=9282436 (last accessed 14.10.22).

terrorist organisations is catered for under the broader policy 'Violent or graphic content policies'[763].

- Poland-based JustPaste.it's Terms of Service forbids the posting of unlawful material in the user's country of residence, including terrorist content defined by reference to the offences specified in the European Union's Directive (EU) 2017/541 on combating terrorism, or offences in Member States, or groups or entities designated by the EU or UN[764].

- Dailymotion's Terms of Use contain a reasonably developed list of "terrorist contents" that are forbidden, subject to this being exceptionally maintained on the service because of manifest education, documentary, scientific or artistic context, with the possibility of age-filters[765].

- Twitter has a 'Violent organisations policy' which bans the promotion of terrorist organisations and bans the promotion of terrorism or violent extremism; but subject to the Twitter making exceptions at its discretion for groups that have recently reformed or engaged in a peaceful resolution process, as well as those with members who have been elected to public office[766]. Its 'Violent threats policy'[767] and 'Hateful conduct policy'[768] are also relevant.

- Reddit's short policy 'Do not post violent content' does not refer to terrorist organisations at all, but prohibits 'Terrorist content, including propaganda', but allows that there are sometimes reasons to post violent content "(e.g., education, newsworthy, artistic, satire, documentary, etc.)" [769].

- Discord's short 'Community Guidelines' do not refer to terrorism or terrorists at all, but bans "the organisation, promotion, or support violent extremism"[770].

[763] https://support.google.com/youtube/answer/2802008?hl=en&ref_topic=9282436 (last accessed 14.10.22).
[764] https://justpaste.it/terms (last accessed 14.10.22).
[765] https://legal.dailymotion.com/en/terms-of-use/#prohibited-content (last accessed 14.10.22).
[766] https://help.twitter.com/en/rules-and-policies/violent-groups (last accessed 14.10.22).
[767] https://help.twitter.com/en/rules-and-policies/violent-threats-glorification (last accessed 14.10.22).
[768] https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy (last accessed 14.10.22).
[769] https://www.reddithelp.com/hc/en-us/articles/360043513151 (last accessed 14.10.22).
[770] https://discord.com/guidelines (last accessed 14.10.22).

- Google states in its 'Content policies for Google Search' that it does not "allow content that promotes terrorist or extremist acts, which includes recruitment, inciting violence, or the celebration of terrorist attacks" without further elaboration[771].

- WordPress's policy 'Terrorist Activity' prohibits US designated terrorist groups from using its services and "genuine calls for violence against individuals or groups"[772].

12.34. In the least developed, or absent, category:

- Telegram's FAQ do not disclose any policy on removing content, and states that it does not process any takedown requestions for Telegram chats and groups which are private. However, for public activity (e.g. channels and bots) it invites users to alert it to abuse, including by Islamic State/ ISIS (a further short post says that Telegram's abuse team "actively bans ISIS content on Telegram"[773]) and draws attention to EU takedown requests for terrorist content[774].

- Gab's Terms of Service make no reference to terrorism but states that user contributions must not be unlawful or in furtherance of an unlawful purpose (under US law), unlawfully threaten or incite imminent lawless action[775].

- TOR (The Onion Router, a way into the dark web) says in its 'Legal FAQ' that it is not designed or intended to break the law but that its developers have no ability to prevent illegal activity that may occur through TOR relays[776]. There is no content moderation policy.

Automation and Lists

[771] https://support.google.com/websearch/answer/10622781?hl=en#zippy=%2Cdangerous-content%2Cterrorist-content (last accessed 14.10.22).
[772] https://wordpress.com/support/terrorist-activity/ (last accessed 14.10.22).
[773] https://t.me/isiswatch/2 (last accessed 14.10.22).
[774] Under EU Regulation 2021/784.
[775] https://gab.com/about/tos (last accessed 14.10.22).
[776] https://community.torproject.org/relay/community-resources/eff-tor-legal-faq/ (last accessed 14.10.22).

12.35. Writing in 2019[777], the (now former) head of CT at Facebook explained that its policy team did not take part in most removals: that was down to machine-learning classifiers and a team of more than 15,000 reviewers (dealing with all content, not just terrorist content: only 200 of these were specialists on terrorist groups and other dangerous organisations). Flagging content internally was found to be much more accurate that user reports of abuse; government reports and reports from "trusted flaggers" were generally precise but much less voluminous.

12.36. Given the scale of removals (14.3 million pieces of content related to Islamic State, Al-Qaeda or their affiliates), it is obvious that there are "limitations" on the capacity of human moderators, assuming any are employed at all, once material has been identified for consideration[778]. In the 3 months April to June 2021, YouTube says that it removed 5.9m videos (of which 431k concerned promotion of violence and violent extremism) by automated flagging, dwarfing all other sources of detection[779].

12.37. In 2019, the technical options were[780]:

- Content matching (digital fingerprints or 'hashes' of known bad files). Lists[781] created by membership organisations (see below) provide a means of pooling knowledge on hashes (such the GIFCT's list[782], or the Terrorist Content Analytics Platform run by Tech Against Terrorism, said to be the world's largest database of verified terrorist content[783]), and the Home Office provides a filtering list[784].
- Optical recognition technology scanning for logos or weapons.
- Hashtag tracking.
- Machine-learnt text classification

[777] Fishman, B., supra.
[778] As well as the risk of personal bias, exposing moderators to endless amounts of violent material has a human cost. However, some teams dealing with terrorist material may be highly motivated (as is reportedly the case of police officers who look for child sex abuse material).
[779] https://www.youtube.com/howyoutubeworks/progress-impact/responsibility/#detection-source (last accessed 14.10.22).
[780] Fishman, B., supra.
[781] Of course lists are in principal open to abuse: 'OnlyFans accused of conspiring to blacklist rivals', BBC News (22.2.22): claims that a pornography site procured the inclusion of its rival's content on a counter-terrorism database used by tech companies; or error.
[782] In 2021 it was reported that because it only included hashes of images or videos it excluded pdfs of terrorist manifestos.
[783] TCAP Report, supra.
[784] Potential drawbacks with lists include, if widely circulated, facilitating evasion techniques by terrorists.

- (for encrypted content, but with a high error rate) behavioural analysis.

12.38. Each of these techniques carry drawbacks. For smaller companies, there may simply be the cost element. For the individual, they may find lawful material removed because or errors in mechanical assessment – such as the removal of thousands of videos documenting atrocities in Syria by YouTube, where the individuals concerned are unlikely to have access to other means of distributing or even storing content[785]. This places a premium on appeal mechanisms and transparency[786].

12.39. One of the fundamental policy decisions faced by tech companies is how to determine who is a terrorist[787]. The former Facebook executive identified the following options:

- Rely on international designation lists produced by the UN or EU. Whilst this allows companies to harness collective wisdom and sidestep difficult policy choices, lists are the product of political consensus and are updated slowly. UN lists are dominated by Islamist terrorist organizations, meaning that extreme right wing groups or individual terrorists are not included.
- Use designation lists produced by governments. However, this inevitably forces companies to choose between governments, based typically on whether they are democratic.
- Designate terrorists themselves, with all the analytical and competence questions that arise.

12.40. These complexities are compounded by the difficulties in determining whether content has been produced by a listed organisation or not. Islamist content is often easier to determine as official because of the use of branding and established media outlets. ERWT material is more likely to be supporter-generated than branded[788].

12.41. A further option to rely on the assessments of membership organisations.

Membership Organisations

[785] Macdonald, S., Correia, S., & Watkin, A. (2019). Regulating terrorist content on social media: Automation and the rule of law. International Journal of Law in Context, 15(2), 183-197.
[786] Ibid.
[787] Fishman, supra; Meserole, C., Byman, D., 'Terrorist Definitions and Designations Lists' (RUSI, 2019).
[788] Tech Against Terrorism, TCAP Report (2022), page 15.

12.42. The two membership organisations discussed in this section occupy a hybrid position, having combined characteristics of tech companies, governments, and civil society. As well as a practical coordinating function, for those who distrust the commercial judgments of tech companies, or the political motives of governments, they provide a source of alternative authority for judgements on individuals, groups or content.

- It is difficult to exclude the role of governments. Governments have their own information and capabilities and may have operational observations about removing content or websites.

12.43. Involvement by tech companies is entirely voluntary. There are positive and negative aspects to this. Some companies may be more willing to cooperate, knowing that they retain control, and find it easier to communicate with tech insiders than with governments or regulators; but others will happily opt out.

12.44. It is unclear how membership, and acceptance of membership criteria, interact with members and conditions/community standards. I have not seen any tech company terms and conditions which expressly state that they will moderate content in line with lists or assessments compiled by membership organisations.

GIFCT

12.45. The Global Internet Forum to Counter Terrorism is a membership organisation founded by and appealing to larger tech platforms.

- It provides a database of terrorist content (hashes), a facility for members to share suspect weblinks (URLs), and a Critical Incident Protocol for responding quickly to real-world terrorist content such as attack live-streaming[789].
- Various governments including the UK, the US and EU Member States play a role in its governance as part of an Independent Advisory Committee[790].
- It has a research arm, the Global Network on Extremism and Technology[791].

[789] See ISC, REF, at 267 to 269.
[790] https://gifct.org/governance/ (last accessed 17.10.22).
[791] https://gifct.org/research/ (last accessed 17.10.22).

12.46. At the time of writing, its membership among larger tech companies is impressive but not comprehensive (total of 19 members; neither TikTok or Telegram are members)[792]. For some companies, membership is incompatible with their stance on content moderation, because a requirement of GIFCT membership is an explicit prohibition of terrorist activity. As set out above, Telegram bars the promotion of violence only on publicly viewable channels whilst many particularly smaller platforms do not expressly ban terrorist content at all[793].

12.47. Smaller companies may also lack the capacity to demonstration compliance with the GIFCT criteria for membership[794].

12.48. The database of terrorist content (hashes) is available to some but not all members[795]. It is based on:

- Content 'related to' organisations on the UN Security Council Consolidated Sanctions List (in practice, Islamist Organisations)[796].
- Content arising from ad hoc attacks which engage the Critical Incident Protocol, currently the ERWT attacks at Christchurch and Halle (Germany), and the incel-related attack in Arizona in 2020[797].

Tech against Terrorism

12.49. Tech Against Terrorism is a UK-based initiative supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED) and was launched in April 2017. It is funded by GIFCT and, to date, by the governments of Spain, Republic of Korea, Switzerland, and Canada[798].

[792] https://gifct.org/membership/ (last accessed 17.10.22).
[793] Macdonald, S., Rees, C., S., J., 'Remove, Impede, Disrupt, Redirect: Understanding & Combating Pro-Islamic State Use of File-Sharing Platforms', CYRTEC (Apr 2022).
[794] https://gifct.org/membership/ (last accessed 17.10.22).
[795] However, in 2021 only 14 of its members had access to it: GIFCT Transparency Report (2021).
[796] It is foreseeable that GIFCT may come under some pressure not to use a group-based approach in future. Its Human Rights Assessment (BSR, 2021) at p35 stated that there was near consensus among experts and stakeholders that terrorist content should be defined by reference to behaviour rather than groups because of the risk of stigmatising associated communities. This overlooks the fact that the UK (at least) is keenly aware of this risk in any decision on proscription.
[797] Ibid. For the Arizona attack, see 'Self-Proclaimed 'Incel' Gets 44 Years After Filming Himself Committing Arizona Mall Shooting' (Oxygen, 12.7.22).
[798] https://www.techagainstterrorism.org/project-background/ (last accessed 17.10.22).

- There are eight requirements for membership[799].
- It also aims to secure the involvement of small tech companies, by offering a simplified 'pledge' which to be achieved "…as quickly and thoroughly as possible, consistent with available resources and scale"[800], and through mentorship.
- The prize for members is access to interactive tools and resources, such as lists of terrorist logos, terms, phrases, and templates for terms and conditions[801].

12.50. There is an impressive focus on transparency and detailed analysis, going beyond mere research, which attempts to identify, through inclusion in a Terrorist Content Analytics Platform, content whose removal is justified[802]. At present this is:

- Content created by designated Islamist and Extreme Far Right Terrorist organisations.
- There are 18 designated Islamist groups and listed Islamic State and Al-Qa'eda affiliate groups, as designated by democratic states and the UN or EU.
- Here content means official, not supporter-generated, material.
- There are 13 designated Extreme Far Right Terrorist organisations, as designated by member states.
- It is unclear whether relevant content under this heading also extends to supporter-generated material, or only official content.
- The Christchurch livestream and manifesto, the Brievik manifesto, and the Buffalo livestream and manifesto. In each case this turns on designation by the New Zealand government. I consider the options for designating content in the UK, below.

12.51. The stated ambition is to include other terrorist groups from other ideological strands, to increase the pool of designated Islamist and ERWT terrorist groups, to include supporter-generated material, and further lone-actor content[803]. The platform has recently encompassed content created by neo-Nazi James Mason, author of the

[799] https://www.techagainstterrorism.org/membership/trustmark/ (last accessed 17.10.22).
[800] https://www.techagainstterrorism.org/membership/pledge/ (last accessed 17.10.22).
[801] 'Knowledge Sharing Platform': https://ksp.techagainstterrorism.org (last accessed 17.10.22).
[802] https://www.terrorismanalytics.org/policies/inclusion-policy (last accessed 17.10.22).
[803] Ibid.

woefully influential 'Seige'[804], and based on his listing as a designated entity by the government of Canada[805].

12.52. Identifying and removing terrorist operated websites is another aspect that TaT has targeted[806]. This is different from content removal – it targets websites based primarily on their operators. TaT aims to provide an assessment service so that tech companies can make informed decisions on whether to continue to host[807].

UK Input

12.53. There are arguments in favour of the UK playing a greater role in identifying objectionable terrorism content (either by reference to content itself, or the groups or individuals who produce it). As a democratic nation, with especial competence in counter-terrorism, UK decisions are likely to feed through into content moderation by tech companies and inform lists and assessment produced by membership organisations.

12.54. This can help shore up the accuracy and legitimacy of content moderation generally. It could be said that the UK should be in a position to play a full part in signalling terrorism content, rather than having to rely on designations by other democratic states.

12.55. However, it can also be argued that the UK authorities would be unwise to take on a role that they cannot fairly and accurately accomplish:

- The volume of potentially radicalising material is too large to monitor.
- Any positive decisions could only ever be taken reactively and depend upon where the focus had fallen, for example because it had arisen in criminal cases, or had been reported by a member of the public or in the media.

[804] See e.g. Johnson, B., Feldman, M., 'Siege Culture after *Siege*: Anatomy of a Neo-Nazi Terrorist Doctrine', ICCT (July 2021).
[805] https://www.terrorismanalytics.org/project-news/new-TCAP-entity-James-Mason?utm_source=Tech+Against+Terrorism&utm_campaign=351945a2d6-EMAIL_CAMPAIGN_2022_05_27_COPY_01&utm_medium=email&utm_term=0_cb464fdb7d-351945a2d6-184139337 (last accessed 17.10.22).
[806] 'The Threat of Terrorist and Violent Extremist-Operated Websites' (Jan 2022).
[807] 'Responding to Terrorist Operated Websites' (Jul 2022).

- It would be impossible to achieve consistent and equitable decisions across the range of potential material.

12.56. To assume this burden could also encourage tech companies to divest themselves of the responsibilities that they have so recently accepted.

Section 3 Terrorism Act 2006

12.57. This power permits a police officer to "require" a service provider to prevent identified material no longer being available online[808]. However, it has no effective enforcement mechanism and, unsurprisingly, has never been used. Published guidance on the use of section 3 (of which I have a copy[809]) is no longer available online.

12.58. In principle, it applies to material that is "unlawfully terrorism-related" which means, in summary, material that is likely to be understood as an encouragement to terrorism or likely to be understood in its form or context as being wholly or mainly useful for terrorist acts[810].

12.59. However, the only effect of the "requirement" is to remove one of the defences that is available in a prosecution of the service provider under section 1 (encouragement) or section 2 (dissemination). Where a "requirement" has been served, the non-endorsement defence which in principle allows a person who is responsible for recklessly publishing or disseminating terrorism content to argue that it did not have their endorsement[811], is no longer available[812].

12.60. Although sections 1 and 2 Terrorism Act 2000 can both be committed by a person outside the UK[813], it is unlikely that CT Police would be inclined to give a

[808] Section 3(3)(b).
[809] With thanks to Professor Clive Walker QC.
[810] Section 3(7).
[811] Section 1(6) and 2(9).
[812] Section 3(2). At one stage I wondered whether the Electronic Commerce (EC Directive) Regulations 2002 provided a further defence for service providers which were 'mere conduits' or provided cashing or hosting services, as suggested by paras 33-7 of the Guidance. However, the Regulations, which implement the eCommerce Directive 2000/31/EC, and provide a further line of defences only applied to existing legislation (see Reg 3(2)). Moreover, since the Directive did not apply to services based outside the EU (see recital (58)), the principles in the Directive would not apply in the case of most service providers.
[813] Section 17 Terrorism Act 2006, as amended by the Counter-Terrorism and Border Security Act 2019.

section 3 requirement to an overseas company. Despite being designed with overseas companies in mind[814], it seems that Parliament cannot have fully considered the ramifications of seeking to enforce UK terrorism standards against overseas providers based, in most cases, in the US. For completeness, section 3 would not be an effective mechanism in respect of the administrator or moderator of a website who refused to remove unlawfully terrorism-related material[815].

12.61. It follows that section 3 is the wrong mechanism for the UK to signal to tech companies which content is beyond the pale. The heavy implication of the withdrawn guidance was that voluntary cooperation should always be sought, and that is in practice how CTIRU[816] have operated.

12.62. Moreover, a requirement by a police officer, however well-informed, would not carry the democratic imprimatur of measures such as proscription or (sanctions) designation, and it cannot be guaranteed that tech companies or membership organisations would regard a section 3 requirement as having equivalent legitimacy.

12.63. In last year's annual report, I recommended that criminal courts should be given a power to refer certain content to the police for them to consider whether to exercise their section 3 power[817]. In its response, the government has stated that it wishes to consider my fuller consideration of terrorism online in this year's report.

12.64. There was considerable sense in that response, since having had a longer opportunity for research and reflection, I see no useful purpose would be served by conferring such a power on criminal courts where the section 3 power is clearly a hollow measure. I do not recommend repeal of section 3 itself, but only because I think it preferable to wait to see how the legislative landscape lies after the enactment (or not) of the Online Safety Bill. However, I return to relevant decisions of the criminal courts below.

Alternatives

[814] Section 4 provides for services on companies registered outside the UK.
[815] The activities of an administrator or moderator do not fit within the activities listed in s2(2), and in any event an omission to remove content created by a third party would not amount to conduct that might encourage a third person within the meaning of section 2(1) Terrorism Act 2006.
[816] For CTIRU, see Chapter 1.
[817] Terrorism Acts in 2020 at para 3.32.

12.65. **Proscription** of terrorist organisations under the Terrorism Act 2000 provides the UK's main influence over content moderation by tech companies, particularly because the UK has been quick to proscribe Extreme Right Wing Terrorist organisations which lie outside the ambit of UN and US designation lists. However, as explained in Chapter 3, it has its limitations and does not apply to individuals or content.

12.66. **Financial counter-terrorism sanctions**[818] are available against individuals as well as groups and carry a reasonable degree of procedural protection[819].

- As amended by the Economic Crime (Transparency and Enforcement) Act 2022, the threshold for designation is reasonable grounds to believe a person's involvement in terrorism (including by promoting or encouraging it[820]).
- The effect of designation is to impose limitations on providing finance, entry to the UK and military goods and technology[821]. It might be questioned whether imposing these types of restrictions on individuals is the right category of response if the sole purpose is to send a signal to tech companies about associated online content.
- For example, if an individual published a terrorist manifesto, the objective might be to secure its permanent removal from the internet, but the impact of sanctioning its author would (if he had assets in the UK) have a greater impact on that individual, financial institutions and third parties that mere content removal

12.67. However, sanctions have been used imaginatively in the online context. The Russia (Sanctions) (EU Exit) Regulations 2019 were amended in April 2022[822] to require social media service providers from encountering *content* generated by designated persons[823], as part of a programme of trade sanctions.

[818] Under the Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019 and the Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019.
[819] Under the Sanctions and Anti Money-Laundering Act 2018.
[820] CT Sanctions 2019 reg6 (as amended by the 2022 Act, s61); International CT Sanctions 2019 reg6 (as amended by the 2022 Act, s61).
[821] Under the International CT Sanctions 2019 (the CT Sanctions 2019 are financial only).
[822] By the Russia (Sanctions) (EU Exit) (Amendment) (No.9) Regulations 2022.
[823] Reg.54A(1).

12.68. In other 5-Eyes countries too, financial sanctions have been used where it could be said that the only practical consequence would be to affect designation lists held by tech companies and membership organisations.

12.69. In New Zealand, Brenton Tarrant was designated by the Prime Minister as a "terrorist entity" under the Terrorism Suppression Act 2002 following the Christchurch attack[824]. This is equivalent to sanctioning[825].

- The statutory threshold for potential designation in New Zealand is belief on reasonable grounds that the entity (which may be an individual or a group[826]) has knowingly carried out or participated in one or more terrorist acts[827]. There are no published criteria relating to the Prime Minister's discretion to designate, but guidance suggests that the "guiding consideration" is whether designation "would effectively assist the suppression of terrorism"[828].
- A press release from the Prime Minister's Office provides some indication of why the discretion was exercised: for condemnation purposes[829] and preventing Tarrant from being involved in terrorist financing in future[830].

12.70. In Canada, the US neo-Nazi James Mason was listed as a terrorist entity under the Criminal Code (as amended by the Anti-Terrorism Act 2001)[831]. The Canadian Criminal Code permits an entity to be placed on a list based on knowing involvement in terrorist activity[832].

---

[824] 'Statement of Case to Designate Brenton Tarrant as a Terrorist Entity', https://www.police.govt.nz/sites/default/files/publications/statement-of-case-brenton-harrison-tarrant.pdf (last accessed 21.7.22).
[825] The 2002 Act was principally enacted to enable New Zealand to fulfil UN sanctions and other treaty obligations: see section 3.
[826] Section 4(1).
[827] Section 22.
[828] New Zealand Police, 'The legal framework and process for terrorist designations', https://www.police.govt.nz/sites/default/files/publications/terrorist-designations-process-legal-framework-paper-03-10-2017.pdf (last accessed 21.7.22).
[829] "Designating the offender is an important demonstration of New Zealand's condemnation of terrorism and violent extremism in all forms": Prime Minister, Press release (1.9.20).
[830] "This designation ensures the offender cannot be involved in the financing of terrorism in the future": ibid.
[831] The entry for James Mason, Public Safety Canada, 'Current listed entities' (listed 25.6.21) cites him and Seige as the ideological foundation of 2 UK proscribed organisations, Feuerkrieg Division and Sonnenkrieg Division.
[832] Para 83.05

12.71. As already discussed in this chapter, New Zealand's designation of Brenton Tarrant and Canada's sanctioning of James Mason have been used as inclusion criteria on Tech Against Terrorism's list of terrorism content. There is a case for considering whether UK designation under the counter-terrorism sanctions could, assuming it had the purpose of "furthering the prevention of terrorism in the United Kingdom or elsewhere"[833], be used in a similar way.

12.72. More exotically, New Zealand's **Chief Censor** used powers to ban content created by Tarrant under the Films, Videos and Publications Classification Act 1993:

- By a decision dated 18 March 2019, the Chief Censor concluded that the livestream was "objectionable" on multiple grounds including the promotion of extreme violence, cruelty and terrorism[834].
- By a further decision on 23 March 2019, Tarrant's manifesto was also classified as "objectionable". The Chief Censor noted that whilst it was not likely to be persuasive or harmful to most adult readers, there was a "high risk" of the publication persuading some young people and vulnerable adults, and "the very real possibility" that a small number might be persuaded to act[835]. Subsequent events proved this correct.
- The effect of classification as "objectionable" is to open the door to criminal liability for producing, disseminating and so on under the 1933 Act.

12.73. The Chief Censor used these powers in respect of the Breivik Manifesto[836], the Halle livestreaming and associated instructional material[837], an online game based on the Tarrant attack[838], and the livestreaming and manifesto of the Buffalo, New York, attacker[839]. These have the benefit of being decisions about specific content.

[833] Reg 4(1)(b) of the International CT Sanctions 2019.
[834] Chief Censor, 'Notice of decision under section 38(1): Christchurch Mosque Attack Livestream' (18.3.19).
[835] Chief Censor, 'Notice of decision under section 38(1): The Great Replacement' (23.3.19).
[836] https://www.classificationoffice.govt.nz/news/news-items/white-supremacist-manifesto-banned/ (last accessed 18.10.22).
[837] https://www.classificationoffice.govt.nz/news/news-items/two-terrorist-publications-banned/ (last accessed 18.10.22).
[838] Ibid.
[839] https://www.classificationoffice.govt.nz/media/documents/20220614_Buffalo_proactive_release.pdf (last accessed 18.10.22).

12.74. However, being decisions that are neither taken by an elected official[840] nor subject to Parliamentary debate, there is a question mark over their democratic credentials. The same problem arises over any content-specific decisions that may need to be taken by OFCOM under the Online Safety Act (which I consider further below).

12.75. Nor is the 1933 Act a terrorism-specific legal instrument – it applies to a whole range of video content that is objectionable on grounds such as the portrayal of torture, sexual cruelty, or bestiality[841] - meaning that tech companies or membership organisations must select which banned content to include within its terrorism-specific lists.

12.76. Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 was enacted in the wake of the Christchurch attack[842], and places obligations on internet service providers and others with respect of audio and/or visual material produced by terrorists, murderers, torturers, rapists and kidnappers[843].

- However, the effect of these obligations, if not complied with, is to expose the service provider to criminal liability (together with legal presumption in any future prosecution).
- It therefore suffers from the same deficit as section 3 Terrorism Act 2006, in that it depends upon the willingness of the Australian authorities to prosecute (most likely) overseas service providers.

12.77. Finally, two Australian states have recently emulated Germany and criminalised the display of Nazi symbols[844].

12.78. Although I do not recommend it, it would be possible to frame a novel power to permit the UK greater influence over content moderation lists. For example, the Home Secretary could be empowered to designate a category of internet content (for example, equivalent to Australia's Abhorrent Violent Material) which is "unlawfully

[840] The Chief Censor is an independent Crown entity.
[841] Section 3.
[842] Parliament of the Commonwealth of Australia, Explanatory Memorandum to Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019.
[843] See also Attorney General's Department, 'Abhorrent Violent Material Act Fact Sheet' (16.7.19).
[844] (New South Wales) Crimes Amendment (Prohibition on Display of Nazi Symbols) Act 2022 No 37; (Victoria) Summary Offences Amendment (Nazi Symbol Prohibition) Act 2022 No. 29.

terrorism-related" (as defined by section 3 Terrorism Act 2006) for terrorism prevention purposes; such an order could, like proscription under the Terrorism Act 2000, be subject to Parliamentary resolution.

12.79. The reason I do not recommend the creation of a further power is that, at present, there is no evidence that such a power is currently needed. As shown by the survey above, different democratic nations have a range of differing designation powers which between them seem to be providing a satisfactory basis for content moderation. In addition, there is the possibility that existing UK CT sanctions regimes could be used against individuals, with the reasonable possibility that associated content (such as manifestos) will find their way onto moderation lists.

12.80. However, returning to convictions by criminal courts:

- I have been authoritatively informed that tech companies are prepared to remove content that breaches UK terrorism legislation.
- There is currently no ready means of proving to tech companies which material falls the wrong side of the line.
- This is even though terrorist publications and material that is likely to be useful to a terrorist are frequently found by the criminal courts to form the basis of criminal liability.
- This means that despite a criminal court in Scotland finding Sam Imrie guilty of possession of information likely to be useful to a terrorist in the form of manifestos by Brenton Tarrant and Anders Brievik[845], there is no clear record of this illegality to which CT Police or Tech Against Terrorism or GIFCT can point.

12.81. The benefit of a clear published list of material that has formed the basis of section 2 Terrorism Act 2006 or section 58 Terrorism Act 2000 convictions would go beyond assisting tech companies and membership organisations in understanding the boundaries of UK terrorism law. It would be a resource for journalists and civil society and members of the public to understand what material led to criminal liability, and possibly to put further pressure on tech companies.

[845] See further Chapter 10.

12.82. CT Police are well-placed to compile a record, overseen for quality control purposes by the CPS, of documents that have formed the basis of criminal liability. This is information that is already in the public domain because it will have formed the basis of criminal proceedings (and may well have been covered in the media) and would not involve disclosure of any sensitive information.

12.83. I therefore **recommend** that a formal list is created and published by CT Police of content whose possession or dissemination has led to convictions in the United Kingdom under section 2 Terrorism Act 2006 or section 58 Terrorism Act 2000.

Online Safety Bill

12.84. The progression from the Green Paper (2017) to Online Harms White Paper (2019) to Draft Online Safety Bill (2021) to introduction of the Online Safety Bill (March 2022) to uncertainty (marooned for a long time at Report stage) to heavily amended Bill before the House of Lords illustrates both the complexity of engineering a model of state regulation of the internet[846], and its political sensitivity.

12.85. In its current form, the Bill applies to services that enables content generated, uploaded or shared by one user to be encountered by another user (user-to-user services) or that allows users to search more than one website or database (search services). The remit is far wider than terrorism.

12.86. It is understandable that the Bill should focus on content because tech companies have much greater ability to control content than the behaviour of users. The mechanism selected for defining "terrorism content" is to rely on a list in Schedule 5 of offences under the Terrorism Act 2000, the Anti-Terrorism, Crime and Security Act 2001, and Terrorism Act 2006, and provide that terrorism content is content that "amounts to" an offence under Schedule 5[847].

[846] The lawyer and author Graham Smith's has produced an excellent series of blogs as 'cyberleagle'. 'Reimagining the Online Safety Bill' (18.8.22) contains a summary of difficult aspects of the bill, aside from the category 'legal but harmful'.
[847] Clause 52(5).

12.87. The initial explanation in the Bill for how content could ever "amount to" a terrorism offence lacked coherence because it failed to cater for states of mind or potential defences[848]. This has now been rectified[849].

12.88. However, the problem remains that content and criminal conduct (to which the offences in Schedule 5 are directed) are different[850].

12.89. The seductively simple phrase, "What is illegal offline should also be illegal online"[851], is unobjectionable if it recognises that online activity confers no protection from national and international law.

- But, outside a few rare exceptions, content is not inherently unlawful.
- Whether conduct amounts to a terrorism offence requires a deep analysis of the facts and circumstances surrounding that conduct, most of which will be hidden from view from service providers: for example, whether a statement is said with ironic intent or is being communicated between individuals with a legitimate interest.
- Identifying whether online conduct amounts to a terrorism offence is not always straightforward as a matter of law (as illustrated by the discussion of the encouragement offence[852] in Chapter 7).

12.90. The regulator, OFCOM, appears destined to make finely-tuned decisions on terrorism content. Requiring OFCOM to monitor compliance with systemic safety duties does not ultimately relieve it of having to decide, in respect of particular items of content, whether a tech company has satisfied its safety duties or not[853].

12.91. There is a legitimate question whether, if service providers were willing and able to remove the content identified (for example) in Tech Against Terrorism's Terrorism Content Analytics Platform, any real benefit would derive from requiring them to take additional individual decisions on content:

[848] Hall, J., 'Missing Pieces: A Note on Terrorism Legislation in the Online Safety Bill' (20.4.22).
[849] Clause 170.
[850] The position of terrorism was barely considered in the Joint Committee on the Draft Online Safety Bill's Report of Session 2021-22 (HL Paper 129, HC 609).
[851] See for example, Council of the EU, Press Release on Digital Services Act (25.11.21); Damian Collins MP (chair of Joint Committee on draft Online Safety Bill), Hansard HC vol.718 col.164 (12.7.22).
[852] Section 1 Terrorism Act 2006.
[853] Smith, G., 'The draft Online Safety Bill: systemic or content-focused?' (Inforrm, 3.11.21).

- OFCOM's assessment of the response by video-sharing platforms to the livestreamed Buffalo attack, as regulator under Part 4B Communications Act 2003, was broadly positive; its observations concerning the continuing evolution of industry collaboration and the possibility that "no single model can provide a comprehensive solution" do not suggest that it has any certainty about what is needed.
- It remains to be seen what OFCOM's Code of Practice on terrorism content, to be issued under clause 37(1), recommends: it might do no more than endorse use of lists provided by GIFCT or Tech Against Terrorism.
- The implication of the government's latest Transparency Report[854] is that the regulator's firmest response is to require the use of automated technology in identifying and removing illegal terrorist content[855]: it is difficult to see how this could operate other than using a pre-determined list.

12.92. Throughout this annual report I have drawn attention to the impact on children being drawn into online terrorism.

12.93. However, the Online Safety Bill provides no special measures relating to children and the potential impact of exposure to terrorism content. Surprisingly, although the Bill does create special statutory duties relevant to "content that is harmful to children", this category expressly excludes terrorism content. In July 2022 I published a Note which sets out the law and questioning why terrorism content was exempted in this way[856].

12.94. Failing to require service provides to carry child-centred assessments means less attention to influential terrorism content on platforms most likely frequented by children. For the purposes of counter-terrorism it enables tech companies to treat children as adults, even though the terrorist arrest figures and day-to-day experience of CT Police demonstrate the disproportionate impact that online terrorism content has on children.

12.95. Without specially heightened protection for children from the impact of terrorism content, the protections for children will have to come from generic obligations flowing

[854] 'Transparency Report: Disruptive Powers 2020' (2022) CP 621.
[855] At page 33.
[856] 'Response to first OFCOM consultation re Online Safety Bill' (29.7.22).

from Codes of Practice which will require higher standards of protection for children in relation to all harmful content[857], from duties in relation to 'content depicting or encouraging violence'[858] or content which 'presents a material risk of significant harm to an appreciable number of people'[859]. The special risk that terrorist content poses to children is not recognised, and great faith is placed in the willingness and ability of tech companies to capture terrorism content by performing their generic duties fully.

12.96. Child-specific duties in the field of terrorism content could require:

(a) proper assessment of *where* children are particularly likely to come across terrorism content.
(b) greater focus of limited human and technical resources by tech companies on access by children to terrorism content. As I have already noted, there is often a profound gap between the terms and conditions governing the content that *should* be available on platforms, and the actual removal of offending content.
(c) age-gating on adult platforms which are most conducive to terrorist content, or the removal of hooks on these sites that are aimed at drawing in children[860].
(d) tweaks to recommendation algorithms that target children.
(e) publication of child-specific terms and conditions or policies that reflect the particular harm that is risked to children from terrorism content. These could tilt the moderation appetite so that material which was on the boundary, and should not be removed for adult users, might be properly removed from sites heavily used by children[861].

12.97. Imposing a higher duty on service providers in respect of children and terrorism content recognises that children are susceptible and too often end up bearing the risk. Unfortunately, that is not how the current version of the Online Safety Bill is drafted.

[857] Schedule 4 of the Bill.
[858] Clause 54 enables the Secretary of State to designate content that is harmful to children. An indicative list has been published which includes 'content depicting or encouraging violence'.
[859] Clause 54(4)(c).
[860] Dunckley, V., 'How the Tech Industry Uses Psychology to Hook Children', Psychology Today (24.10.18).
[861] Boundary-straddling material is considered by Davey, J., Comerford, M., Guhl, J., Baldet, W., Colliver, C., 'A Taxonomy for the Classification of Post-Organisational Violent Extremist & Terrorist Content', Institute for Strategic Dialogue (2021).

13. ANNEX: RECOMMENDATIONS AND RESPONSES TO PREVIOUS RECOMMENDATIONS

In **this year's report** I make 8 recommendations.

Chapter 4

13.1. CT Police should establish a new practice for dealing with unexpected LPP material, consistent with the Attorney General's Guidelines on Disclosure, that does not involve the locking down of the entire device [4.65].

13.2. Improved guidance on 'auditors' and the use of section 43 Terrorism Act 2000 powers should be issued to police forces in England and Wales [4.82].

13.3. Consideration should be given to whether individual forces should be required to report on their use of section 43, for publication in official statistics [4.83].

13.4. The Code of Practice on the use of Schedule 5 Terrorism Act 2000 powers of search and seizure in urgent cases should be amended to specify that journalistic material should not be seized or viewed [4.97].

13.5. Steps should be urgently taken to exempt Interpol biometric holdings from the NSD regime under Part 1 of the Counter-Terrorism Act 2008 [4.108].

Chapter 7

13.6. A new child violence diversion order should be considered in cases of children arrested on suspicion of committing terrorist offences [7.88].

13.7. Schedule 4 Modern Slavery Act 2015 should be amended so that all terrorism offences are excluded from the ambit of the section 45 defence [7.133].

Chapter 12

13.8. A formal list should be created and published by CT Police of content whose possession or dissemination has led to convictions in the United Kingdom under

section 2 Terrorism Act 2006 or section 58 Terrorism Act 2000 in order to assist tech companies with content moderation decisions [12.83].

Three recommendations from my report **Terrorism Acts in 2018** had not previously received a final response (whether acceptance, or rejection):

- Concerning the use of remote night-time monitoring of Schedule 8 Terrorism Act 2000 detainees to avoid sleep disturbance [5.27]. The police have now considered whether remote monitoring (alone) would be sufficient and have concluded that it would be unsafe because of the risk of false assurance that a detainee is safe and well. On that basis physical checks are required: the updated Authorised Professional Practice Guidance from the College of Policing requires physical checks to be carried out sensitively.
- Concerning the use by Independent Custody Visitors in Northern Ireland of the form at appendix 2 of the ICVA training manual for custody visitors in England and Wales [5.24]. I am pleased to report that the form in Northern Ireland has now been updated and disseminated for use by the Northern Ireland Policing Board. Although not identical to the form in England and Wales, it is now adequate for use by TACT visitors.
- Ensuring that any time spent in detention following PACE arrest is deducted from the maximum time for which individuals can be detained under section 41 Terrorism Act 2000 [5.29]. The government has now accepted this recommendation in substance and I understand will be bringing forward legislation.

There was one outstanding recommendation in **Terrorism Acts in 2019**:

- Concerning the publication of first instance judgments on Schedule 5 Terrorism Act 2000 production orders in respect of journalistic material [4.51]. I understand that the practicalities are still under consideration.

I made 17 recommendations in last year's report **Terrorism Acts in 2020**. The Secretary of State formally responded to these recommendations in a response laid before Parliament on 31 January 2023.

- The Home Office and CT Police should give consideration as to how to ensure that statistics on the use of terrorism powers can continue to capture useful information about ethnicity (1.11). ACCEPTED

- The use of “Chinese or other” as an ethnicity category in CT statistics should be reconsidered so that it more accurately reflects the individuals within that category (1.13). ACCEPTED

- Consideration be given to publishing the statistics for “White Irish” individuals stopped under Schedule 7 (1.13). ACCEPTED

- The Home Secretary should provide greater clarity over how the five public discretionary factors in favour of or against proscription under section 3 Terrorism Act 2000 operate against predominantly online groups (3.10). REJECTED

- Legislation should be enacted to enable a court sentencing an individual for a terrorism or terrorism-connected offence to recommend that the power in section 3 Terrorism Act 2006 be exercised by a constable (3.32). FURTHER CONSIDERATION

- Information on complaints about the exercise of Schedule 7 should be routinely captured from all police forces across the United Kingdom (6.27). ACCEPTED

- National Counter-Terrorism Policing HQ should analyse ethnicity categories for those subject to tasked examinations compared to untasked examinations (6.34). ACCEPTED

- Paragraph 8 of Schedule 7 to the Terrorism Act 2000 should be amended to enable the proportionate searching and copying of remotely held data, to be accompanied by an amended Code of Practice (6.48). ACCEPTED

- Counter-Terrorism Police immediately establish a new standalone public policy on CT intelligence management which explains, as far as is consistent with national security, how data obtained from Schedule 7 is managed, reviewed, retained or deleted. The policy should explain what controls there are on access to this data and what, if any, oversight there is on the integrity of the retention regime (6.68). ACCEPTED

- The Code of Practice should be amended to refer to the above new policy (6.68). ACCEPTED

- The Home Office and MI5 should formulate general internal guidance on evaluating risk reduction during the currency of a TPIM (8.25). PARTIALLY ACCEPTED

- The Home Office should, in cases involving neurologically atypical individuals, consider whether the attendance of a psychologist at TRGs may be useful when evaluating risk and measures to reduce risk (8.29). ACCEPTED

- An order should be made under section 11(6) Legal Aid, Sentencing and Punishment of Offenders Act 2012, exempting TPIM proceeds from the criteria referred to in that section (8.35). REJECTED

- PSNI's published statistics should include all arrests under section 41, not just those related to the 'security situation' (9.35). REJECTED

- PSNI should not take account of public perception when deciding on the appropriate arrest power for terrorist-related activity (9.45). REJECTED

- The Director of Public Prosecutions for Northern Ireland should seek an authoritative ruling from the court, at the earliest opportunity, on whether the terrorist sentencing guidelines issued by the Sentencing Council in England and Wales or the Scottish Sentencing Council should be considered (not followed) for the purpose of sentencing terrorism cases in Northern Ireland (9.80). ACCEPTED

- Paragraph 20 of Schedule 8 should be amended so that the power to take fingerprints applies with consent at a port in Scotland (10.16). ACCEPTED

E02876111

978-1-5286-3961-3