Scanning the Horizon: Technology and Risk (22 January 2020)

Jonathan Hall QC
Independent Reviewer of Terrorism Legislation

1. My last predecessor but one, Lord Anderson, invoked a nautical metaphor when he spoke of the need to shield the compass. He was referring to fighting terrorism without defeating the law, by keeping to a true set of bearings and principles even when circumstances are hard[1].

2. I am no sailor, but even landlubbers can be attracted to the horizon. The question I want to ask is, how far ahead to new terrorism legislation should the UK be looking? How much time should we spend looking at the horizon?

3. Well the majority of my role as Independent Reviewer of Terrorism Legislation is quite rightly nothing to do with horizons. It is prosaically about existing laws and how they are day-to-day, sometimes day-and-night, operated by officials, their effectiveness, their impact on members of the public, their unintended consequences. I've referred to terrorism legislation but the rules that govern this world are multiple and overlapping, sometimes obscure and many of them - such as Home Office circulars, standard operating procedures, and internal guidance - have nothing to do with Parliament, but nonetheless govern how counter-terrorism is actually practiced in the real world.

4. So, in my forthcoming annual report *of course* I refer to the Acts of Parliament that give counter terrorism officers exceptional powers such as taking biometric samples from people travelling through ports and borders without the need for any suspicion at all[2]. But I also refer to the instructions issued to individual officers telling them how to exercise those powers. These can be just as important.

5. It follows, if you like, that the principal role of the Independent Reviewer is to not look at the horizon, but to go back and walk slowly along the shore, getting sand between their toes, looking in all the rockpools, and to leave horizons and definitely blue sky thinking to others.

---

[1] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2013/04/SHIELDING-THE-COMPASS1.pdf.
[2] Schedules 7 and 8 to the Terrorism Act 2000.

6. So I am wary about looking too far ahead at what terrorism legislation might be needed. But given this invitation to speak here I thought it might useful to consider two broad aspects of terrorism.

7. First, technology. Second, the management of known sources of risk; or using terms that were much ridiculed at the time but have proven surprisingly useful, 'the known knowns'.

8. So far as the first is concerned, we know how disruptive and transformative technology has been on our lives, and the case for looking at legislative reform is considerable.

9. So far as risk, and what reduces risk, is concerned, as some of you may know I was appointed yesterday to conduct an independent review of managing terrorist offender risk under what is known as MAPPA. This is a sort of statutory partnership between police, prisons and probation, with input from other agencies. I'll say a little about this, but because I am at the start of the process I will stick to broader points at this stage.

10. Incidentally, if you've come for a talk about treason – I apologise. I hope this will be considerably more interesting.

11. **Technology.** I want to talk about 5 different areas.

12. **Firstly**, end to end encryption, encrypted metadata[3] and auto-destruction of communications are here to stay. Although advances in de-encryption are constantly being made, it is quite possible in the near future that terrorism investigations will be defeated by suspects withholding passwords meaning that police cannot obtain access to electronic evidence of attack planning or terrorist publications or the like. Either that, or there will be pressure to increase the amount of time individuals can be held in detention before charge[4].

13. From my contact with police in the heat of investigations, it is questionable whether the existing law provides an adequate framework for deterring individuals from refusing to allow access to information on their devices.

14. There *is* a general offence of failing to comply with a special requirement[5]. But the requirement may only be imposed if it can fairly be said that all other

[3] For example using "DNS-over-https".
[4] 14 days under Schedule 8 to the Terrorism Act 2000, paragraph 36(3)(b)(ii).
[5] Section 49 Regulation of Investigatory Powers Act 2000.

methods have been tried[6] and on the basis that there is some likely benefit if access is granted[7].

15. The truth is that these preconditions may be difficult to establish, especially when counter-terrorism police are working against the clock in relation to multiple individuals and multiple devices, where those individuals are in pre-charge detention and must be either charged or released unconditionally[8]

16. It seems to me that Parliament might consider that a refusal to hand over encryption keys during a terrorist investigation, when a clear requirement has been made and with the benefit of legal advice, is a cause of harm which ought to be capable of prosecution and punishment, in the same way as failing to cooperate with a Schedule 7 examination (which may also require provision of a password) or indeed failing to respond to a notice issued in the course of a serious fraud investigation[9].

17. If that is right, a clear and workable offence seems sensible; and is a preferable alternative to longer and longer periods of pre-trial detention being sought as investigators grapple with more and more sophisticated encryption.

18. **Secondly**, there is a need to establish a new statutory framework for biometrics as it affects terrorism legislation. An Australian think tank called the Biometrics Institutes lists 15 types of biometrics including voice patterns and gait analysis[10]. Frankly, I suspect that is a very conservative estimate. The Biometrics Commissioner Professor Paul Wiles, who reviews among other things national security determinations of biometrics obtained under the Terrorism Act 2000 has already commented on the absence of up-to-date legislation[11]; the case for reform was acknowledged in the Conservative party manifesto at last December's General Election[12].

---

[6] Section 49(2)(d) requires that, "…it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section".

[7] Code of Practice for Investigation of Encrypted Information, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742064/RIPA_Part_III_Code_of_Practice.pdf, at paragraphs 3.39-41.

[8] There is no power to bail individuals arrested and detained under section 41 and Schedule 8 Terrorism Act 2000.

[9] Section 2 Criminal Justice Act 1987.

[10] https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

[11] *Annual Report of the Biometrics Commissioner* (March 2019), at paragraphs 15 to 18.

[12] At page 19, referring to empowering the police "…to safely use new technologies like biometrics and artificial intelligence, along with the use of DNA, within a strict legal framework."

19. Amazingly, the Terrorism Act 2000 only contemplates the biometrics of DNA and fingerprints[13]. As with drones, it is obvious that advances in biometrics bring benefits to counter terrorism as well as challenges. For example, in time and with the right safeguards it could be used to enhance terrorist watch-listing at ports and borders. It also has disadvantages. In his review of investigatory powers, Lord Anderson referred to the "fear of surveillance"[14] and if you read last week's reports from South Wales about facial recognition, it seems that Cardiff City football fans agree[15].

20. So a clear and transparent framework with proper safeguards is good for human security in its broadest sense, and good for national security because there will be justified innovations that should not be stifled because the law is too unclear.

21. **Thirdly**, I suspect that pressure will only increase for new laws on searching data rich devices, especially mobile phones.

    a. Terrorism legislation, like other law enforcement laws, is cast in terms that are suited to searching rooms and searching bookshelves for physical evidence, but not suited to electronic evidence. What it means to obtain, copy, retain and destroy are quite different when it comes to electronic data. It will be interesting to see the Law Commission's report on search warrants when it is published later this year. For terrorism this particular affects Schedule 7 which empowers counter-terror police to search and copy an individual's entire phone or computer.

    b. This has particular relevance to the protection of privileged or journalistic material. Some parts of terrorism legislation do not deal adequately with how, when privileged or journalistic material is bundled up with a mass of electronic data, police can review what they need, whilst protecting what they have no right to see. If a model is required, there is much to value in the Investigatory Powers Act 2016 which talks in terms of access and selection for examination which more clearly reflects how police deal with masses of electronic data[16].

22. **Fourthly**, there is the possibility of legislating against at least a certain category of violent extremist material. This is not strictly speaking an online problem but seems to be coexistent with it. The debate on this issue is right in

[13] Schedule 8 Terrorism Act 2000, paragraph 20A et seq.
[14] Lord Anderson QC, Report of the Bulk Powers Review (2016), at paragraph 9.2.
[15] https://www.walesonline.co.uk/news/wales-news/protest-against-police-using-facial-17554862.
[16] For example, section 263(1) defines destruction as making access impossible.

the open after the Coroner of London Bridge inquests questioned whether a new offence was justified[17]. In her evidence to the inquests, Khuram Butt's wife accepted that her husband not only had pictures of mass killings but also forwarded them to her and his sister[18]; moreover, police were aware at least of Butt's possession of these images some months before he carried out the attacks[19].

23. I have made some suggestions on my Twitter account and received a range of stimulating responses. The main point from those responses, and I think first question to be answered is whether a new *terrorist* offence is needed at all. To be candid, when I was appointed I was surprised to find that possession of execution or torture videos was not already an offence. But then I was also surprised to learn of a Canadian website which until it was shut down hosted images of murders, suicides and tortures and was said to receive 10 to 15 million visits per month. There is a need – and this is particularly relevant to the next part of my talk – to be careful who is labelled as a terrorist offender.

24. If you are interested it is possible that a model based on the extreme pornography offence[20] would provide a possible framework for identifying the sort of material whose very possession should be an offence. It is also worth looking at the Australian attempts to deal with first person shooter videos like the footage of the Christ Church massacre[21] which suggests any new offence has to be tightly drawn with reference to the most extreme violence.

25. But I think there remains a question of whether what is needed is an offence which widens the sort of material that cannot be distributed, or an offence which can be committed merely by possession. Whatever the case, there is an absolute need to avoid legislative overreach: journalists, and those trying to draw attention to human rights abuses must be protected.

26. **Finally**, a word about terrorist groups. Organisations with physical presence are one thing; what if an organisation operates entirely online, so that it is difficult or impossible to identify members or leaders, and where participants may well not know each other's real names, never meet in the offline world, and may not live in the same country? Does the current law allow the proscription (even assuming it would be desirable) of loose networks of online groups, especially in the right wing terrorist sphere? When Israel recently updated their terrorism laws, they adapted the definition of terrorist

[17] London Bridge Report on Action to Prevent Future Deaths at paragraphs 67-8.
[18] Day 21, page 58.
[19] Day 19 pages 55, 97-98; Day 20 pages 13-18, 23.
[20] Section 63 Criminal Justice and Immigration Act 2008.
[21] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019.

organisation with a view to meeting this challenge[22]. This is definitely one to watch: the importance to the authorities of being able to proscribe a group should not be underestimated, as the experience of Al Muhajaroun has shown.

27. **So turning to the second part of my talk: Known knowns**. The focus of anxiety after the London and Manchester attacks of 2017 was known unknowns – those on fringes (closed subjects of interest as they used to be called) or unknown unknowns (especially low sophistication self-starters). Society contemplated the possibility that anyone might be a terrorist: a phenomenon Professor Clive Walker termed Neighbour Terrorism, heralding the dystopian arrival of All-Risks Policing[23]. But as I will go on to say, it is neither possible nor desirable to attempt to eliminate every risk.

28. The cohort that I want to speak about are those already identified by the authorities as terrorists. I refer to three categories - those identified as aligned to Da'esh overseas who may eventually return to UK; convicted terrorists who are still in prison but as we know from recent events may present a continuing risk even whilst incarcerated; and convicted terrorists who have been released.

29. This is of course not a popular group, which is why retaining a sense of balance and fairness when formulating new laws is particularly necessary as well as challenging. But even before you get to questions of balance and fairness there are prior utilitarian questions that cannot be dodged - what works? It is I think important to understand the scale and the nature of the phenomenon.

30. Such understanding involves honesty all round. It is often said that terrorist recidivism is very low but that is in the sense of reconviction - what about the scale of re-engagement in terrorism-related activity that is not prosecuted? My sense is that policy makers need greater long-term visibility of the impact of measures which means sharing of intelligence by MI5 and police even after the end of any overt intervention. That is true both as a matter of 'what works' and as a matter of 'what is justified'.

31. On the other hand, there is a need to disentangle terrorism as an act (against which society must be protected) from terrorism as an offence. Many terrorist offences are what are known as pre-cursor crimes (for example possession of a document, or providing funds to a proscribed group) which do not in themselves result in immediate terrorist violence but which are nonetheless justifiably penalised. It is an inevitable irony that the hallmark of a successful

[22] The Counter-Terrorism Law, 5776-2016, Article 2(a).
[23] Neighbor Terrorism and All-Risks Policing of Terrorism, Professor Clive Walker QC, Journal of National Security Law & Policy [2009] vol3:121.

counter-terrorism operation - keeping people safe from harm in the short term and therefore getting in early before a really serious offence has been committed - may limit the amount of disruption in the long term because there may only be evidence for prosecution of a less serious offence.

32. For this category of offenders the sentences will continue to be modest - so discussion of making terrorists serve their full sentences should not overlook the reality that many terrorists will be released sooner or later even if they do serve their full sentence. Similarly, it must be recognised that what makes an individual progress from terrorism in its broadest sense to acts of violence is poorly understood.

33. Turning to individuals overseas, any affiliation with Da'esh is of legitimate concern to society both in terms of accountability for crimes that may have been committed, and the risks presented by those individuals both overseas and on return. But dividing overseas travellers into a cohort of fierce Foreign Terrorist Fighters and Jihadi brides is too crude. As there are different terrorists, so there are different individuals who went to join Da'esh. Calling all women Jihadi brides by portraying them as passive victims of males in some cases risks underplaying female agency[24]; the law does not quite deal, I think, with those who provide important moral but not material support[25].

34. Different individuals will have different risk and activity profiles. In particular any crude categorisation avoids an honest look at the most difficult group, the so-called children of the Caliphate for whom the starting point must be that they are victims, whatever risk they also present.

35. As for individuals so for remedies. Prison does not affect all individuals equally and it may well be that for some individuals prison "…increases their status in the network and prolongs their activism"[26]. It may also provide a perfectly receptive and captive audience for recruitment. This is an issue that even affects the US, whose prisons are sometimes considered a model of harsh effectiveness. Last December a Texas court convicted a serving terrorist prisoner at the Federal Correctional Institute in Beaumont, Texas. He was already serving a sentence for attending an Al Qaeda training camp in

[24] There has been a notable change of approach in Germany; see https://www.europarl.europa.eu/RegData/etudes/STUD/2018/621811/EPRS_STU(2018)621811_EN.pdf, 2.3.3.

[25] Although any broader offence would need to be carefully drawn: see the US experience, Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).

[26] What is to be Done about al-Muhajiroun?, Michael Kenney (2019), drawing from his book, The Islamic State in Britain, Cambridge, 2018, a study of Al Muhajaroun over time.

Afghanistan in the 90s, but started recruiting fellow prisoners to join Da'esh and carry out attacks[27].

36. That doesn't mean that prison is not the right remedy, but its *consequences* must be addressed, including, as the recent HMP Whitemoor attacks show, recognising that terrorism offending does not stop at the prison door and there is no automatic 'job done' when a terrorist is behind bars.

37. The reason I focus on the known knowns is that it is here that the greatest political risk resides. At a superficial level it is more palatable for an unknown to slip through the net, than for a known terrorist to return to terrorist violence: the desire to insulate from this risk all the greater. In conclusion I offer the following thoughts.

38. Firstly, it is impossible to guard against all risks. Attempting to do so in one case leads at the very least to reduced capacity in another.

39. Secondly, there is no magic test for risk at the point of release[28] - which means that one should be cautious about minimising a trial judge's assessments of risk and seriousness when passing sentence. There are also issues of principle here: a system in which length of sentence was entirely handed over to risk experts would be unacceptable.

40. This is not designed to suggest a counsel of despair.

41. Away from legislation much can be done: for example, smarter sharing of information including sensitive information. One of the terms of reference of my MAPPA review is to consider the adequacy of information sharing between public bodies with very different characters.

42. Existing criminal law, in particular criminal law relating to terrorist radicalisation, can be enforced inside as well as outside prisons.

43. For individuals returning from Syria, there are tools out there such as Temporary Exclusion Orders which (perhaps with some minor changes as I

---

[27] *US v Ahmed* USDC ED Tx 13 December 2019, https://www.justice.gov/opa/pr/federal-inmate-convicted-attempting-provide-material-support-isis; for a UK example see *R v Abdul-Rehman Gul* 21 June 2019, convicted of circulating ISIS propaganda in prison, https://www.independent.co.uk/news/uk/crime/isis-propaganda-prison-jail-young-offenders-gul-phone-a8969821.html.

[28] See for example, the review of literature published by the Youth Justice Board for England and Wales in 2012, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/396030/preventing-violent-extremism-systematic-review.pdf.

suggest in my forthcoming annual report) can be used to address some of the risks.

44. Finally, a few words about the MAPPA review itself. The group of offenders to be considered are offenders convicted under terrorism legislation, those whose offences are considered to be 'terrorism-related', as well as other offenders who have become radicalised or involved in terrorist activity. It also includes considering those who have engaged in terrorism activity whilst in the Prison Estate. In other words, those who have offended and then been released and who are considered to present an enduring risk.

45. The question of whether existing MAPPA structures are adequate, or whether more resources or powers are needed, will require a close look at how things really happen on the ground. But I hope that as many people as have an interest or perspective will be generous enough to share their thoughts.

46. My conclusion is that of course we can look to the horizon, but we must do so with our feet planted firmly on the ground.