“National security: law, political violence, free speech, and subversion.”
(National Liberal Club, London, 2.12.25)

Introduction

2025 has been the busiest year of my 6 years as Reviewer. This year, as well as delivering annual reviews on terrorism and State Threats, I have done special reports on Southport, new laws against state entities like Iran’s Islamic Revolutionary Guard Corps, and on reforming Separation Centres in prisons. I’ve written and spoken publicly about Palestine Action, and given evidence to the Joint Committee on the National Security Strategy about the collapsed China spy trial.

Today I propose to speak for 15 or so minutes and will only be able to touch on the infinite strands that these days fall within or adjacent to national security laws, and then I hope we can have questions and a conversation.

None of what I have just said by way is a complaint about being overwhelmed. Far from it. The expectations on me are largely self-regulated – so long as I deliver my annual reports it’s up to me what other commissions I accept, what media engagements to do, and best of all what topics I pursue. There are now equivalents to me in Australia and Republic of Ireland, but they are more formal, come with more resources but more responsibilities. The strength of the UK role is its freedom and flexibility.

It is impossible for a terrorism reviewer to talk about law and political violence without referring first to Northern Ireland – the fount and origin of domestic laws against terrorism, and still, for all its flaws, home to a successful ongoing process of transition from violence to politics. I recall Sir John’s Major’s tributes to Michael Ancram, at the inaugural Lothian lecture earlier this year, for his patience and commitment to peace in Northern Ireland.

Sir John Major also said that a child today would not recognise life 50 years ago. He was referring to global instability. But he might equally have referred to the greatest gulf between a child of the 1970s and a child today which I will describe as ‘digital life’.

Digital life is central to national security, is not an adjunct consideration, and is not to be categorised and dismissed by drawing analogies with earlier technologies such as television, that have caused moral panics and then become integrated into our lives. To my mind, the online dimension is categorically new.

Consider the fact that children spend more time playing online than they do playing outside with one another, and that on one of most popular online games for children, Roblox, it is possible to enact a school massacre or mosque shooting. Consider the chatbot Sarai that encouraged a man to take a crossbow to Windsor to try and kill the late Queen. Think about Dylan Earl, recently sentenced for a total of 23 years, who was recruited online by the Wagner Group to arrange arson at a warehouse containing equipment destined to support Ukraine. All this is quite apart from the technical opportunities given to adversaries for hostile surveillance, disruption through cyber-attacks, new attack methodologies etc.

I would say that merely recording the fact of our digital life, without dwelling on its profound implications for national security, is a gross error. It would not be strategic, and I found it surprising that the online dimension was not a major thematic in the National Security Strategy published in 2025.

Law

Part of my role as a legal Reviewer is to consider the impact on personal freedoms from laws concerning national security. Sometimes they impact a narrow range of people (for example, in recent times up to 4 people annually have been subject to harsh TPIMs, a type of civil measure to counter dangerous terrorists who cannot be prosecuted), or a broader range (for example, roughly 2,500 passengers have been subject to no-suspicion counter-terrorism examinations at airports and seaports).

Incidentally, for many years legal challenges to this power of examination, known as 'Schedule 7', came from Muslim passengers. It is indeed possible that in a world where Islamist terrorism remains the greatest threat, that unfair and biased assumptions will on occasion be made in deciding who to target. Hence the need for vigilant review.

However, I suspect that challenges are these days just as likely to come from the libertarian right. I am thinking of Tommy Robinson's recent acquittal for failing to comply with a Schedule 7 examination. His acquittal, which I should say made sense on the evidence presented to the court, was funded by Elon Musk; and I foresee similar challenges where police officers, looking for signs of terrorism, run up against free speech advocates.

The broadest counter-terrorism impact is Martyn's Law which was given Royal Assent this year and is due to come into effect after an implementation period of at least 24 months. I continue to have reservations about the regulatory burden of this law which requires tens of thousands of businesses, clubs and charities to have plans for a terrorist attack.

Another aspect relating to personal freedom and counter-terrorism legislation is that people should understand the laws that govern their behaviour and which promise, in the case of national security laws, to protect them. This aspect was recently discussed by a House of Lords Committee on the Rule of Law in a report which is commendable for its lack of jargon and clarity.

Applying this to our digital life, Ministers continue to state that the Online Safety Act 2023 will make the UK the safest place to go online in the world. That's all very well but I can assure you that every day a journalist, a researcher, a police officer, a concerned member of the public will find a piece of terrorism content online that, according to the Online Safety Act simply should not be there. In the last month, for example, my special adviser Adam Hadley found a Facebook account openly identifying itself as affiliated to Islamic State, openly posting an instructional document on the "deadliest places for stabbing" on a body diagram, which had been online for at least a month and remained accessible despite being reported to Facebook itself.

In legal terms this counts as "priority illegal [terrorism] content" under the Online Safety Act and a user-to-user service such as Facebook should have systems to detect, prevent and remove it. The text had obvious keywords for automated flagging: "deadliest", "stabbing", "knife". It was a site openly affiliated with Islamic State.

The short point is that the Online Safety Act relies on tech platforms to apply safety duties. OFCOM's role is to monitor those safety duties but tech companies make it very difficult for regulators or researchers to monitor their output at scale. And nothing in Online Safety Act allows the authorities to take down content or to order tech companies to take it down. But despite this, you will continue to hear Ministers saying that Online Safety Act makes the UK the safest place to be online.

Returning to the relationship between members of the public and the law, I think we need much greater clarity about what the Online Safety Act can and cannot do. Digital life is too important for us to be left in the dark.

Secondly, we need to keep looking at whether proscription – that's the banning mechanism used by Home Secretary, most recently against the groups Palestine Action, Maniac Murder Cult and Russian Imperial Movement – can be adapted without unintended consequences to deal with online movements who venerate lone attackers like Brenton Tarrant or Anders Breivik and inspire copycat attacks but do not amount to organisations.

Thirdly, we need to consider whether our pre-digital laws governing surveillance are unduly restricting the ability of counter-terrorism authorities to consider publicly available information online – that is, information that we have freely publicized and/or surrendered to tech companies for advertising purposes.

Fourthly, however, I think the UK needs to hold its nerve in face of compelling challenges from free speech absolutists, generally based on principles in the US constitution, that in effect consider all regulation of the internet a bad thing. I think that is not only naïve (of course much of the internet is a highly controlled environment, it's just controlled by tech companies and their algorithms) but also ultimately undemocratic because it suggests that we as society through our laws cannot assert control over our digital lives despite the harms, especially to children.

This is why, for all its flaws, I support the principle of the Online Safety Act. Incidentally, the US is no monolith. Individuals States are constantly trying to impose legislation to protect children, but time and time again a body called NetChoice, the trade body for tech companies, succeeds in striking down these efforts on First Amendment grounds.

Political Violence

I want to turn now to political violence. There is a classic debate about whether all terrorism is political (and so whether it is necessary to identify religious racial or ideological causes under the Terrorism Act), but what can be recently observed is violence relating to contested matters of domestic politics which ideally would be resolved through the ballot box and not through violence.

In 2025 a man called Paul Martin was convicted of terrorism at the Old Bailey for trying to lead a violent rebellion against Covid restrictions. In January this year Alexander Dighton stabbed police officer because he considered that the authorities had lost control of the UK's borders. And of course, in the summer, Palestine Action was proscribed whose actions were said to be motivated by views on arms sales to Israel. I might also add that 2025 saw two attacks on think tanks – Policy Exchange earlier this year and Tony Blair Institute only a few weeks ago.

It is tempting, and not necessarily wrong, to draw a link with the 6th Jan attack on the US Capitol in 2021, and with some of the other US political murders in recent times. For the first time, according to a study by eminent scholar Dan Byman of Georgetown University, there are more cases of political violence in the US coming from the Left (think of the attack by Luigi Mangione) than the Right, although Left Wing attacks are less deadly.

Crudely put, these types of attacks can be distinguished from the Islamist Extremist terrorism and neo-Nazism terrorist acts of recent years. What the Islamist Extremists and neo-Nazis want are not matters of domestic debate: a Caliphate or Sharia, a world free of subhuman non-Whites, whatever, are not on offer by any UK or US political party. But things like Covid restrictions, control of borders, and divesting from Israel, are things our politicians agree and disagree about.

This may explain in part why some people find the banning of Palestine Action so difficult – the cause is not as extreme as what motivates Islamist Extremists and neo-Nazis, because what they promote is a matter of genuine debate. That said, I don't think it makes an ounce of difference – it is the methods that are used that matter not the cause.

I'm afraid I draw a rather pessimistic conclusion from this type of violence. It appears to reflect a culture in which participation in mainstream democratic mechanisms such as voting, political parties, think tanks, and of course non-violent protest, are no longer perceived as effective or even legitimate.

Hence the move to direct action under cover of protest. This is an exhausted narcissism where an appeal to the right side of history is a refusal to debate with your fellow man. And none of this is improved if politicians debase the standards of public life by, and I am not referring to politicians in the UK here, posting falsehoods, playing to extremism, or abusing their office.

Free Speech

I want to return to free speech because it is so central to debates about online safety and therefore the national security. A picture of an Islamic State atrocity is a matter of historical record and can be shared in order to discredit; but it can also be used to recruit followers and encourage attacks.

Our go-to reference point for the free speech debate remains the real world: for example, the Gaza protests, Elon Musk's speech at the 'Unite the Kingdom' rally, or Bob Vylan's "Death to the IDF" chants at Glastonbury. Each of these examples give rise to weighty points of debate and a lecture in their own right.

But generally speaking, the egregious examples of people literally calling for death, or encouraging terrorism, or calling for people to be killed in yet more violent ways, or to end their own lives, or to go and carry out sabotage for the Russians, are to be found online.

And here, we are, I suggest, still floundering in the shallows. We have yet to achieve a mature analysis of the role and value of online speech.

First of all, in the online domain it is *not* the case that more speech is remedy for bad speech, as proposed by JS Mill and famously applied by Justice Brandeis of US Supreme Court. It is not a marketplace of ideas but an echo chamber where positions are generally hardened not exposed as falsehood or lacking nuance.

Secondly, online disinformation is easier, cheaper, less accountable (think of anonymous accounts) and possibly more effective (think of deep fakes). The pervasiveness of false information is potent enough to change some of the calculus on how much weight and respect should be given to online speech as a whole. Imagine a student was told that 50% of all factual assertions in books in a law library were false.

Consider this extract from a recent paper by Sam Stockwell from the Alan Turing Institute. He was writing about the run up to Australia's federal election in May 2025. A Russian-linked influence network published a large volume of fake news stories promoting pro-Kremlin narratives. The purpose of this – and here it becomes very interesting - was "to attract the search engine crawlers used to build AI chatbots – thereby distorting the data these tools draw on to produce responses that promoted Russian interests". It was found during tests that "nearly 17% of the chatbots' answers amplified these false narratives – demonstrating the moderate gains attackers could make using this relatively cheap technique."

I think that we need a JS Mill for the online age.

Finally, in considering the difference between real speech and online speech, there is a point to be made about the mode of counteraction. Countering terrorist content online generally means removing the electronic signals that make up the content. Stopping speech in real world must generally be done through arrest or prosecution, or the threat of arrest or prosecution, all of which carries a greater impact on individuals.

Subversion

I'll end with subversion. We don't exactly need it, but a very recent KCL survey reported by the Times found an increase in sense of national division and loss of pride in country.

A major aspect is once again the online dimension. In the words of the Telegraph's Tim Stanley, algorithms pushing division are "a technological development that has aligned with (or caused or hastened) the collapse of 20th-century political norms." To pull some optimism from this catastrophic assessment, I am glad that the UK legal system, which is not based on absolutist notions of free speech, allows us to do something about this before it is too late.

As much as it is important to be realistic, it is important not to talk up division. The collapse of the West is one of the key Russian themes that the Kremlin promotes directly or through the dark PR firms it employs. It would also play nicely into China's vision for a world order if we junked democracy and reached for the strongman.

You may recall some images of black-clad and masked thugs in the East End the other month. It is possible that this was an Islamist powerplay to dominate the streets (as is too often the case in prisons). But it is also possible that rumours were circulating in the Muslim population about imminent attacks, and that young men came onto the streets in self-defence and in genuine fear. The problem is that we often don't know what other people are seeing in their online feeds and I think we shouldn't be overhasty in judging other people until we know what they believe to be the facts.

One of strengths of terrorism and national security laws is that they are threat-neutral, which allows the authorities to say that our laws are not anti-Islam, or anti-Irish, or indeed anti-White, or anti-China. I think it's more difficult when we get to extremism. We may know it where we see it, but it's hard to come up with an abstract definition.

I confess I tend to run a mile when I see an anti-extremism law but I'll end by saying that countering extremism, or fostering cohesion, or identifying a core set of British values, or encouraging resilience, as part of a wider project to protect national security from subversion, are buoys that we are likely to go around many times in the coming years.

A simpler fix is to make sure different parts of the system talk to one another, as failure of China spy case tends to demonstration. Another is to make sure that organs of democratic life in the UK are protected, within which I include the BBC (given how much the UK's adversaries want it to fail), local media, think tanks, universities, charities and NGOs. But, whatever we do, we need to put the online domain front and centre in the protection of national security.

I will end with an optimistic note. We are in the online foothills, but we will learn and adapt. I think society is becoming much stronger in protecting children from online dangers, and all eyes will be on Australia whose social media ban comes into force in 8 days' time. I think that protecting children is not a bad place to start.