State Threats Legislation in 2024

REPORT OF THE INDEPENDENT REVIEWER OF STATE THREATS LEGISLATION ON THE OPERATION OF PARTS 1 AND 2 OF THE NATIONAL SECURITY ACT 2023 AND SCHEDULE 3 TO THE COUNTER-TERRORISM AND BORDER SECURITY ACT 2019

By JONATHAN HALL K.C.

Independent Reviewer of State Threats Legislation

December 2025

State Threats Legislation in 2024

REPORT OF THE INDEPENDENT REVIEWER OF STATE THREATS LEGISLATION ON THE OPERATION OF PARTS 1 AND 2 OF THE NATIONAL SECURITY ACT 2023 AND SCHEDULE 3 TO THE COUNTER-TERRORISM AND BORDER SECURITY ACT 2019

By JONATHAN HALL K.C.

Independent Reviewer of State Threats Legislation

Presented to Parliament pursuant to Section 63 (6) of the National Security Act 2023

December 2025

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 978-1-5286-6138-6
E 03512978 12/25

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

EXECUTIVE SUMMARY

- This is an independent review in the United Kingdom's legislative response to the malign activities of foreign States below the threshold of armed conflict.

- The United Kingdom has tooled up against these 'State Threats' by granting major new powers to the authorities, updating old spy laws, and creating genuinely novel criminal offences such as 'foreign interference', 'sabotage', 'theft of trade secrets', and 'assisting a Foreign Intelligence Service'.

- Some of the powers and offences extend well into the zone of political activity, journalism, protest and day-to-day human activity. However useful, they must be tested against misuse and overreach.

- I have identified the following areas which will require particular vigilance as these laws are deployed:

    - The power to stop and detain travellers who are unwittingly caught up in State Threat activity at the UK border.
    - The 'Foreign Power Condition', which does not require any contact with a Foreign Power.
    - Innocent interactions with Foreign Intelligence Services.
    - The ability of police to require individuals to leave areas adjacent to Prohibited Places, including in protest cases.
    - The potential impact of the Foreign Interference offence on foreign policy work by think tanks and journalists.
    - Ensuring that the desire to identify and punish State Threat actors does not result in excessively harsh measures against weak, foolish, and inadequate individuals.

CONTENTS

Contents

1. INTRODUCTION

1.1. This Report is an independent review of the national security legislation found in two Acts of Parliament[1]:

- Schedule 3 to the Counter-Terrorism and Border Security Act 2019 ('Schedule 3'). This law confers suspicion-less powers for constables to **examine** travellers at airports, seaports and the Northern Ireland border, and was enacted to fill a "gap" because the equivalent terrorism powers were not considered adequate[2]. With the terminology of its associated Code of Practice referring to 'hostile actors', 'agents' and 'co-optees'[3], this legislation first brought state threats out of the shadows.

- Parts 1 and 2 of National Security Act 2023 ('the NSA)[4]. These establish new and updated criminal **offences**, supporting **investigatory powers**, and a **civil regime** for managing individuals who pose an enduring threat to national security. The NSA is the most important national security legislation since the pre- and inter-war Official Secrets Acts.

1.2. This report is intended to be a standalone report which does not assume and prior knowledge or, or interest in, earlier national security legislation[5].

---

[1] I do not review other national security legislation such as the National Security and Investment Act 2021, the Telecoms (Security) Act 2021, section 29 of the Procurement Act 2023, or Part 4 of the National Security Act 2023 (Foreign Influence Registration Scheme). Nor do I review the powers of the intelligence agencies; sanctions; immigration measures such as deportation or exclusion, or controls on advanced students seeking to study subjects of potential military use (the Academic Technology Approval Scheme); prerogative powers such as passport removal or citizenship deprivation.

[2] Hansard (HL) Vol 793 Col 1701 (12.11.18), Baroness Williams, Minister of State.

[3] Annex C.

[4] Excluding section 30 which contains a special criminal defence for members of United Kingdom intelligence services and armed forces. Part 3 sets up the powers of reviewer. Part 4 contains the Foreign Influence Registration Scheme (not in force in 2024). Part 5 makes amendments to terrorism legislation.

[5] For example, the Official Secrets Act 1911, which has been repealed by the Act and is now only of relevance to conduct taking place before 20 December 2023 when the Act came into force.

1.3. Although the harm at which Schedule 3 is directed ("hostile state activity") is expressed differently from the target of the NSA ("foreign power threat activity[6]"), both regimes serve the same cause. That is, to harden the United Kingdom as a whole[7] against the **malign activities of foreign states below the threshold of armed conflict** in the same way as the Terrorism Acts have proven a workable and effective framework to operate against a different threat to national security[8].

1.4. Taken together Schedule 3 and the NSA provide a formidable but, but still largely untested, basis for investigating, prosecuting and deterring state threats.

Assertive Law

1.5. The chemical weapons attack by GRU officers[9] at Salisbury in 2018 and its effect on the United Kingdom's national security posture cannot be understated.

1.6. Russia had been assertive, and it was time for an assertive response[10]. There would be a "pivot" in the national security apparatus towards dealing with state threats[11]. The government promised to invoke "the wider levers of state power" to combat diverse and wide-ranging state threats[12].

---

[6] Despite its title, "national security" is not an important feature of the Act.
[7] Schedule 3 and the NSA apply UK-wide; cf. Hendriks, M., Halem, H., 'Rediscovering Northern Ireland's Role in British National Security' (Policy Exchange, 2024). The Act extends with modifications to the Sovereign Base Areas of Akrotiri and Dhekelia: The National Security Act 2023 (Sovereign Base Areas) Order 2024.
[8] HM Government, Consultation: State threats legislation (July 2020).
[9] The GRU is a unit of Russia's military responsible for special or unconventional operations: Watling, J., Danylyuk, O., Reynolds, N., 'The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022-24' (RUSI, 2024).
[10] Intelligence and Security Committee, Russia Report (2020) at para 19; HM Government, IR2023, Integrated Review Refresh, at para 16.
[11] P.F. Scott, 'State threats', security, and democracy: The National security Act 2023' *Legal Studies 2024; 44(2):260-276.*
[12] HM Government, Integrated Review Refresh (2023), at paragraph 14.

1.7. Legislation is one component[13]. No longer would the UK make-do-and-mend with outdated official secrets[14] and terrorism legislation[15]. The function of MI5, "the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means"[16] would be brought out of the shadows and given flesh by conferring powers on the authorities and duties on citizens.

1.8. By design:

- The potential for overt intervention by law enforcement is increased by new powers and criminal offences.
- Foreign officials involved in hostile activity, and their foreign and British civilian accomplices, are at greater risk of detection, arrest and prosecution.
- Where states are involved in *any* criminal conduct this can be publicly exposed in court.

1.9. The United Kingdom would become a "hard operating environment"[17] against State Threats, defined by MI5 as "overt or covert actions by foreign governments which fall short of direct armed conflict with the UK but go beyond

[13] Another is greater public messaging, such as the Interference Alert issued in respect of Christine Lee and the United Front Work Department in 2022.
[14] The Official Secrets Act 1911 to 1939. In 2020 the Law Commission reported on the need for updating legislation in its Protection of Official Data Report (HC716, Law Com No 395).
[15] The use of Schedule 7 in the case of smuggled UK intelligence material, upheld by the Court of Appeal in R (Miranda) v Secretary of State for the Home Department and Commissioner of Police for the Metropolis [2016] EWCA Civ 6; the use of section 58 Terrorism Act 2000 against Magomed-Husejn Dovtaev for carrying out hostile reconnaissance for the benefit of Iran: Daily Telegraph, 'Terror scout caught spying on broadcaster's London base' (20.12.23).
[16] Section 1(2) Security Service Act 2023.
[17] National Security Act 2023, Explanatory Notes at para 7.

peaceful diplomacy and expected statecraft to harm or threaten the safety or interests of the UK or our allies"[18].

1.10. Increased assertiveness against foreign actors and their accomplices means greater *personal risk* to malign individuals; more *embarrassment* for states who are caught out; and new *counter-intelligence* opportunities.

1.11. The goal of assertiveness in the widest range of situations underpins three key aspects of the legislation.

1.12. **Firstly**, and borrowing from threat-neutral terrorism legislation, the law applies to activity on behalf all foreign states equally, those who are considered friends and 'frenemies' as well as enemies[19].

- Technology has made it easier for a wider range of states to damage UK interests.
- More countries are willing to use state threats as an aspect of statecraft.
- States are more interconnected through crucial supply chains, meaning ever more complex dependencies.
- This may also be relevant to "false flag" operations, where agents of a generally hostile state secure an individual's cooperation by pretending to be agents of a friendlier sate.

1.13. There is no limit as *how* threats may be generated by states: through their intelligence services, organs such as China's United Front Work

[18] MI5 website, 'Countering state threats' (last accessed 25.9.24).
[19] The Law Commission had recommended abolishing "enemy" as an outdated concept: HC716, supra, at para 3.14 et seq.

Department[20], diplomats[21], other state officials, proxies[22], or indeed any person acting for the foreign state's benefit[23].

1.14. **Secondly**, unlike terrorism legislation with its foundational definition[24], the NSA avoids exhaustive and therefore potentially limiting global definitions[25] in the face of complex and always evolving threats[26].

1.15. There is a wide field to defend: since 2021, government strategy has referred to a new focus on tackling state threats to the United Kingdom's democracy, economy[27] and information[28] (particularly with reference to China) and society, and protecting its science and technological base[29].

1.16. Rather than identifying a target harm (for example, undiplomatic activity, or covert, clandestine or coercive conduct by agents of a foreign power) and penalising different manifestations (for example, violence, threats, funding etc), the NSA is built around a typology of state threats (for example, spying, sabotage, foreign interference) with the implicit prospect of further types of threats being penalised at a future stage without reference back to a unifying feature.

---

[20] Exposed in the Australian foreign interference prosecution of Di San Duong: sentencing remarks of HHJ Maidment, Melbourne County Court (29.2.24).
[21] See for example, Khoshnood, A.M., Khoshnood, A., 'The Islamic Republic of Iran's Use of Diplomats in Its Intelligence and Terrorist Operations against Dissidents: The Case of Assadollah Assadi (2024) 37 International Journal of Intelligence and CounterIntelligence 976.
[22] MI5 website, 'Countering State Threats' under 'Who poses a threat?'.
[23] See the Foreign Power Condition examined in Chapter 2.
[24] Terrorism is defined in section 1 Terrorism Act 2000.
[25] For example, further definition of prejudice to the safety and interests of the United Kingdom was thought undesirable because of the need for flexibility: Hansard HL Deb, vol 826, cols 972–973, 19 December 2022 (Lord Sharpe of Epsom).
[26] On mutating threats, see Director General of Australian Secret Intelligence Organisation, 2023 annual threat assessment.
[27] See Erie, M. 'Property as national security' (2024) Wisconsin Law Review.
[28] Sir Richard Moore, Chief of MI6, speech (Prague, 19.7.23).
[29] HM Government, Integrated Review Refresh (2023), at paragraph 3(ii). China under the Chinese Communist Party has presented a challenge "across almost every aspect of national life and government policy"

1.17. A different legislative path might have been taken. In 2019, Schedule 3 established border powers based on a formulation of "hostile state activity" underpinned by reference to national security[30].

1.18. But a deliberate decision was taken to avoid this terminology in future legislation including the NSA[31]. In addition, criminal legislation built around a vague notion of national security might be widely applicable, but it would far from certain and so contrary to general principle[32].

1.19. **Thirdly**, the policy of the legislation is plainly to exclude loopholes, particularly those that might arise from the use of technology.

- Cyber activity and remote access and temporary malfunction are covered through tech-proof language and wide extra-territorial jurisdiction.
- Formalities are avoided[33].
- Defences are largely absent, no doubt to avoid gaming of the legal system.

1.20. **Fourthly**, the legislation is not just aimed at deliberate threat actors but, in the case of the NSA, at those who "reasonably ought to known" that they are caught up in malign activity; and in the case of Schedule 3, at individuals who may be entirely unwitting of the damage they are risking. The general public, accessible to all online, are potential participants on the field of play but

[30] Paragraph 1(6).
[31] The phrase is ambiguous. Is it hostile activity or activity by hostile states? The government recognised the risk of confusion in Home Office, 'Consultation Document: Legislation to Counter State Threats', updated 12 July 2022. In addition, since all states including the United Kingdom carry out intelligence and influence activities abroad, it can be doubted "hostile" the right word to describe such activity.
[32] National security is not defined in legislation. In Secretary of State for the Home Department v Rehman [2001] UKHL 47, [2003] 1 A.C. 153, "national security" was held to mean simply "the security of the United Kingdom and its people", per Lord Hoffman at para 50.
[33] For example, espionage (section 1) does not depend on the stolen material being protectively marked: HM Government, Human Rights Memorandum for NSA, at para 16 (cf. the further reference to "loopholes" at para 10).

especially those with knowledge (academics), skills (ex-military) or lack of inhibition (ordinary criminals)[34]. The authorities have already directed threats at enablers ("…we will bring the full weight of the national security apparatus down on you"[35]) and it is likely that the authorities will use successful prosecutions as public lessons[36].

Rights and Freedoms

1.21. It is unavoidable that national security legislation hoists a flag for police involvement in broad reaches of human endeavour, with the risk of damaging mistakes by investigators and unjustified suspicion being cast on lawful activity.

- Because national security is not just about explosive acts of sabotage or intrusion into military bases, hitherto lawful conduct, such as relations with foreign intelligence officers or participation in paid influence campaigns, are potentially in scope.
- It is as possible to misread the intentions of individuals, as it is the interests of states.
- Sophistication and disguise are hallmarks of State Threat activity.
- Roles such as journalists and lawyers, ordinarily accorded special protection in a democracy, may be deliberately exploited as cover.
- The legislative intent of avoiding loopholes increases the risk of innocent conduct being caught, putting the onus on investigative and prosecutorial discretion.

[34] As to Russia's crowdsourcing use of criminal proxies, see Richterova, D., Grossfeld, E., Long, M., Bury, P., 'Russian Sabotage in the Gig-Economy Era, (2024) The RUSI Journal, 169:5, 10-21.
[35] Director General MI5, Threat update (8.10.24).
[36] Much as Operation Crevice (R v Amin and others, 2004) was seen as an opportunity to educate the public about the risk from Al Qaeda and Islamist terrorism.

1.22. In their communication[37] on the new article 23 of basic Law of the Hong Kong Special Administrative Region (HKSAR) of the People's Republic of China, adopted on 19 March 2024, six UN Rapporteurs[38] noted the extent to which basic rights and freedoms were threatened by a law supposed to protect national security:

- By suppressing challenge and disagreement on political and constitutional matters[39].
- By conferring excessive discretion on officials, and threatening sanctions, based on vague and undefined notions of "national security".
- By threatening political and journalistic freedoms, intruding into education, and calling in to question engagement with civil society actors and organisations with foreign links.

1.23. It is proper to consider how national security legislation can be abused in the wrong hands[40]. Unless exceptionally well exercised, the UK's novel and wide-ranging powers will result in cases of real harm where an individual is wrongly arrested or investigated, however well-intentioned.

1.24. I recognise that it is possible, owing to the lower profile of State Threats within the general population than terrorism and counter-terrorism, that such instances will pass largely unremarked. Wider attention may be stirred if these new powers are seen to bear down on groups. As the United States later concluded of its own "China Initiative", action against foreign espionage or

[37] OL CHN 5/2024 (Geneva, 22.3.24).
[38] On the promotion and protection of the right to freedom of opinion and expression; the right to education; the rights to freedom and peaceful assembly and of association; the situation of human rights defenders; the independence of judges and lawyers; and the promotion and protection of human rights and fundamental freedoms while countering terrorism.

[40] For example, the targeting of foreign Non-Governmental Organisations by the Russian authorities considered by the European Court of Human Rights in Ecodefence and others v Russia, App.No.9988/13 and others (14.6.22), Third Section.

influence can lead to perceptions of racial profiling[41]. In harness with phases of public anxiety that sometimes arise[42] the very existence of these powers could implant doubts in the public about the lawfulness of relations with foreign nationals.

1.25. In their enthusiasm to expose foreign state activity police and prosecutors must avoid crushing the butterfly on the wheel. Some of those who come through the national security portals, as is increasingly the case with terrorism, are young or inadequate. MI5 has already drawn a direct comparison between criminals who have their strings pulled by foreign states, and those radicalised online[43]. Oddballs are attracted to espionage, hacking, and conspiracy, and State Threat legislation will inevitably scoop up a fair share of these.

1.26. Of course, oddballs, like children, can sometimes cause or threaten serious harm to national security. Failing to protect the United Kingdom from State Threats would in the long run curtail individual rights and freedoms. Unimpeded hostile activity could poison the general the well-being of our society by undermining its military capacity, damaging its economy, and inhibiting personal freedoms such as free speech, including by harming UK-based individuals like dissidents or journalists[44].

[41] NPR, 'The Justice Department is ending its controversial China Initiative' (23.2.22), quoting Assistant Attorney General Olsen of the US Justice Department.
[42] Cf the "Spy Fevers" or "Red Scares" that abounded after the First World War.
[43] Director General MI5, Threat update (8.10.24).
[44] Hansard (HC) Vol 728 Col 49, 'Statement on the security threat to UK-based journalists', Security Minister (20.2.23).

Review

1.27. I was appointed by the Home Secretary as Independent Reviewer in February 2024[45]. The purpose of independent annual review is to allow Parliament to monitor, from an informed position, whether these State Threat laws go too far or, as the case may be, not far enough. It has been described as best international practice[46].

1.28. I hold very high security clearance meaning enabling me to receive tightly held information and maintain contact with officials within government, the intelligence agencies, and the police involved in countering State Threats. I remain a barrister in independent practice and work alone[47]. It is up to me to decide what questions I want to ask and what additional topics I want to consider within my annual report. I operate with complete independence.

1.29. Parliament has allowed the Home Secretary, after consultation with the independent reviewer, to remove any material that would be contrary to the public interest or prejudicial to matters such as national security[48]. If removal is made, she must make a statement to that effect[49].

1.30. My approach will remain as it has for reviewing terrorism: if my report to Parliament is to have any value it must be fully public. If I genuinely cannot say

---

[45] Under section 63 NSA. Prior to 20.12.23, the Investigatory Powers Commissioner was obliged to review the operation of Schedule 3 (see para 62), but that function has now been transferred to the Independent Reviewer, although by section 63(1)(c) NSA, my review into Schedule 3 excepts "…the functions of the Investigatory Powers Commissioner under Part 1 of that Schedule".

[46] OL CHN 5/2024, supra.

[47] Unlike the Commissioner or my Australian equivalent, The Independent National Security Legislation Monitor, I do not have power to compel information from the authorities, nor do I have a staff of inspectors. For the reasons discussed in Hall, J., 'To review or monitor terror laws?' (Counsel, 10.4.23), I do not consider that this has not to date inhibited effective independent review.

[48] Section 36(7) (cf para 62(4) of Schedule 3 for review previously conducted by Investigatory Powers Commissioner). Section 36 Terrorism Act 2000 does not contain an equivalent power, merely a duty for the Secretary of State to avoid prejudicing ongoing criminal proceeding when considering when to lay the report before Parliament.

[49] Section 63(6)(b).

something without risking damage to the public interest, then it has no place in my annual review. It is also no part of my role to provide a legal textbook of flaws and loopholes to hostile state actors.

1.31. The report reviews the National Security Act 2023 and Schedule 3 to the Counter-Terrorism and Border Security Act 2019 as they were enacted. It is separate from my analysis of what additional powers might be needed in 'Legislation to Address State-Based Security Threats to the United Kingdom' (May 2025), a report commissioned by the Home Secretary in December 2024, which also contains a detailed consideration of the relationship between legislation against terrorism and legislation against State threats.

1.32. This report was drafted shortly after the National Security Act 2023 came into force. In my second (and final) annual report, it will be easier to illustrate how the NSA has operated in practice since implementation, because I will be able to refer to prosecutions that are now working through the system. Recognising the newness of the legislation I have only made three recommendations.

Statistics

1.33. There is no equivalent for State Threat legislation of the detailed official statistics available for terrorism legislation in the quarterly Home Office publication, 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation', which also includes details on prosecutions and prisons.

1.34. The only source specifically on State Threats legislation is found in the quarterly Parliamentary reporting on the use of State Threat Investigation and Prevention measures[50].

1.35. Considerable nervousness has been expressed to me about exposing, or appearing to expose, the UK's capabilities to hostile adversaries by publishing details of how counter-terrorism police have exercised their new powers under State Threats legislation.

1.36. I also recognise that the data points of significance in terrorism statistics may be different for State Threats legislation as against terrorism legislation: for example, nationality may be as important as ethnicity, and the identity of the State for which an individual is thought to be acting may be as important as the precise offence for which he has been charged.

1.37. However, it is indisputable that published statistics are invaluable for public understanding and detailed review. They can provide important indications of trends[51], which may require a legislative response from Parliament.

1.38. It is too early to say what statistics will become available. However I **recommend** that the Secretary of State identifies a date before, or a time period within which, official statistics on the use of State Threat powers should be published.

[50] Section 55 NSA.
[51] For example, in the terrorism field, the recent increases in children and young people subject to terrorism-related arrests.

2. CRIMINAL LIABILITY

2.1. Any increased use of criminal proceedings against State Threats as an assertiveness mechanism carries the resource cost of investigating and prosecuting, and the reputational burden of maintaining prosecutorial standards. Deviations from high criminal justice standards will be seized upon by adversaries and diminish the effectiveness of criminal justice outcomes.

Prosecutorial Discretion

2.2. Prosecution of the new offences under the National Security Act 2023 must first be signed off by the Attorney General through the mechanism of prior consent[52].

2.3. This mechanism, requiring a detailed submission from the Crown Prosecution Service to the Attorney General's Office, is an effective means of focussing minds on whether the evidential and public interest tests are met.

2.4. Entrusting discretion to a Law Officer can never be a complete answer to the potential reach of the new offences, applicable as they are in zones of precious human activity such as journalism, protest and politics. It is limited comfort to an individual who is worried about the legality of the conduct that they will never, in practice, be prosecuted for it[53].

2.5. However, my experience of the operation of terrorism legislation, which also covers a wide field and depends on the sensible use of prosecutor discretion,

[52] Section 37, with the exception of the most minor offences.
[53] In K (Age of Consent: Reasonable Belief) [2001] UKHL 41 (at [24]; [2001] Crim. L.R. 993). Lord Bingham observed that "the rule of law is not well served if a crime is defined in terms wide enough to cover conduct which is not regarded as criminal and it is then left to the prosecuting authorities to exercise a blanket discretion not to prosecute to avoid injustice."

is that this discretion is generally well exercised[54], and has lived up to its description by the former Law Lord, Lord Bingham, as a check against "ill-judged or ill-founded or improperly-motivated or unnecessary prosecutions"[55]. Added to this:

- NSA offending will never be volume crime.
- It can be expected that the foreign policy and consequence management implications (e.g. hostile reciprocal action against UK officials) will already have been considered to some degree before the Attorney General needs to approve or not.
- The decision is not a binary one because if a NSA offence is not authorised, a non-NSA offence (for example, actual bodily harm in place of foreign interference, in a case of attacking dissidents) may be available.

2.6. That said, since the government is likely to be particularly interested in NSA prosecutions from a geo-political perspective, the obligation of the Attorney General to act "quasi-judicially and independently of government"[56], even when taking soundings across Whitehall on matters affecting the public interest, is especially acute.

Procedure

2.7. Judges in criminal proceedings are empowered by the NSA to **exclude the public** from any part of criminal proceedings, save for the passing of sentence (section 38) where it is "necessary in the interests of national security". This is a carry-over from previous legislation[57], and relieves the prosecution of the

[54] However, in Terrorism Acts in 2019 at 7.27 et seq I drew attention to YPG-linked prosecutions where the terrorist aspect appeared to be more technical than real.
[55] R v Shayler [2002] UKHL 11 at para 35, an appeal against conviction under the Official Secrets Act 1989.
[56] Framework Agreement between the Law Officers and the DPP [2019].
[57] Section 8(4) of the Official Secrets Act 1920 and Section 11(4) of the Official Secrets Act 1989.

circuitous argument that damaging national security would also damage the administration of justice[58].

2.8. Given the importance of open justice to exposing State Threats as crimes, this is a provision to be handled with much care. Officials will often have tenable arguments to give to prosecutors, for example, based on the principle of 'neither confirm nor deny' or 'jigsaw identification', or invoking the wider ambience of international relations, why privacy is best. But experiments with closed criminal proceedings, in the UK and equivalent jurisdictions, have not always been a success[59].

2.9. The watchword for depriving the public, the media, and the participants of the illuminating light of public disclosure is whether the restriction is truly "necessary". The UK criminal justice system for dealing with the most serious criminal offences is widely respected. Foreign powers whose agents are prosecuted may exploit (in international discussions or on social media) any divergence from ordinary British justice to try and distract from their role.

2.10. Even if the public is not excluded there are lesser measures which may affect the appearance of ordinary justice. What could be described as balaclava justice – hooded officials entering premises, carrying out arrests, designated in paperwork as Officer A, B, C etc, and appearing anonymously in court behind screens with voice modulation – is not a welcome prospect. There are legitimate reasons for increasing courtroom protection for officials and police involved in countering State Threats, but they should be explained to the judge.

---

[58] As explained at Guardian News and Media Ltd & Ors v R and Incedal : [2014] EWCA Crim 1861 paras 16-17.
[59] In the UK, in Guardian News and Media Ltd & Ors v R and Incedal [2016] EWCA Crim 11, where accredited journalists were admitted into private hearings in an attempt to counter-balance the largely private nature of the proceedings, in which the name of the defendant were initially anonymised; in Australia, the 'Alan Johns' affair, criticized by the Independent Monitor of National Security Legislation, Grant Donaldson SC, in a report dated 17.6.22.

Diplomatic and State immunity

2.11. The failed Iranian Paris bomb plot of 2018 proves the role that accredited diplomats can play in the most violent State Threat activity[60]. However, if accredited in the territory where the conduct takes place[61], a diplomat enjoys personal immunity from arrest and prosecution[62] leaving only the option of expulsion as 'persona non grata', unless that immunity is expressly waived by the sending State. Where it does apply, immunity from criminal suit is personal, and does not absolve co-conspirators. This means non-accredited individuals involved in NSA offences jointly with diplomats may still be prosecuted.

2.12. Unaccredited or 'undeclared' intelligence officers of another state do not enjoy diplomatic immunity and are an avowed target for prosecution under the NSA[63]. State immunity is an additional principle of immunity[64] and is enjoyed by foreign state officials acting in the course of their official work, whether diplomats or not, although probably not when operating in the UK[65].

The Foreign Power Condition

2.13. The principal field of conduct addressed by the NSA is the clash and competition between the UK and other foreign powers. Little wonder then that the foreign power condition in section 31 of the National Security Act 2023 is

[60] Khoshnood, A.M., Khoshnood, A., 'The Islamic Republic of Iran's Use of Diplomats in Its Intelligence and Terrorist Operations against Dissidents: The Case of Assadollah Assadi' (2024) 37 International Journal of Intelligence and CounterIntelligence 976.
[61] Since Assadi was the third secretary to the Iranian embassy in Austria, it was not available for his conduct in France.
[62] Articles 29, 31 Vienna Convention on Diplomatic Relations (1961) given force in UK law by the Diplomatic Privileges Act 1964.
[63] HM Government, Policy Paper, 'New espionage offences: factsheet' (19.8.24).
[64] Immunity from civil proceedings is given under the State Immunity Act 1978, but immunity from criminal proceedings is a matter of customary international law.
[65] See Bat v The Investigating Judge of the German Federal Court [2011] EWHC 2029 (Admin), considering the Forum State exemption.

central to all but four of the new offences[66], to the investigative powers, and the imposition of civil controls on unconvicted suspects[67].

2.14. In short, this special ingredient can transform blameless conduct, or conduct that violates civil law obligations only, or conduct that is criminal but not serious, into matters of national security suitable for investigation, prosecution and control[68].

The meaning of foreign power

2.15. There are essentially three meanings of "foreign power".

2.16. **Firstly**, it means central and regional governments, including government agencies and authorities[69]. This category includes governments of "territories", which are deemed to include constituent territories of a federal State[70], but are otherwise undefined by reference to size.

2.17. **Secondly**, other authorities "responsible for administering the affairs of an area" in a country or territory abroad including persons exercising those functions[71]. This is a complex provision to interpret.

- In isolation, it could be interpreted as including lower tiers of government and other authorities because administering the affairs of an area, at least in the United Kingdom, is generally a matter for shared responsibility between central government, local authorities (delivery of

[66] It does *not* apply to the foreign intelligence service offences (sections 3, 17), and the prohibited places offences (sections 4, 5).
[67] Prevention and Investigation Measures under Part 2.
[68] Scott, P., *supra*. Section 31(7) puts beyond any doubt that the foreign power condition applies just as much to foreign officials as to any other member of the public. The purpose of this provision was to avoid arguments about whether the acts of officials were acts of states.
[69] Section 32(1)(a)-(c).
[70] Section 32(4).
[71] Section 32(1)(d).

adult social care and the provision of rubbish collection) at varying political levels (parish councils, district councils, borough councils, county councils, unitary authorities etc), often involving private companies trusts and charities (responsible for collecting the bins or running private and academy schools or nursing homes).

- However, it would be a stretch to describe every borough council or police force as "administering the affairs" of a territory or region, and it is implausible that Parliament intended every unit of overseas officialdom to constitute a "foreign power".
- One effect of the provision may be to include quasi-State bodies which exercise governmental power, such as the Palestinian Authority in the West Bank of Israel, or, the unrecognised government in Somaliland[72]. In principle it could extend to supranational organisations such as the European Union or (in former times) the Soviet Union.
- In principle this will also include terrorist groups in charge of territory, such as Hamas in Gaza, or the Houthis in Yemen, including groups proscribed under the Terrorism Act 2000.
- However, the effect will also be to capture the broad and often regionally-based structure of the Chinese state, including its intelligence functions, which may well be carried out without central tasking from Beijing[73].

2.18. The question arises of how to classify a foreign police force seeking to intervene covertly in UK affairs. Although such a police force would likely qualify as a Foreign Intelligence Service for two of the NSA offences[74], the possibility cannot be excluded that the Foreign Power Condition will be satisfied in the case of a foreign police force.

---

[72] Other areas where there is territorial control by non-state or unrecognised bodies include Aphazia, Transdenestria, Northern Cyprus, Afghanistan.
[73] Joske, A., 'The party speaks for you: Foreign interference and the Chinese Communist Party's united front system' (Australian Strategic Policy Institute, 32/2020).
[74] See Chapter 3.

2.19. Leaving aside the remote possibility that a foreign police force will qualify as having responsibility for administering the affairs of a territory[75], it is conceivable that the foreign police force will be acting as an *intermediary* for a state. In that case the foreign power condition may be satisfied as it applies to indirect relationships between conduct and states[76]. In addition, an individual who assists a foreign police force with state threat activity may *intend* to benefit the foreign government of the country that the police force serves[77].

2.20. **Thirdly**, a foreign power includes a governing political party, whose members hold government posts, or which is significantly influential over the holder of government posts[78]. In an anthropomorphic view of statehood, the political party comprises the brain of the foreign body politic. Up-and-coming political parties are excluded from the definition, even though they may have once held government power, and may hope to do so again.

2.21. A deliberate decision was taken not to include State-owned companies as a further category[79]. But it is conceivable that a corporation could be the authority responsible for administering the affairs of a country or territory. In the past this was the position of the East India Company; and could arise today if a private military contractor engineered a coup and took over the functions of government.

---

[75] Cf. R v Reeves Taylor [2019] UKSC 51, in which the Supreme Court held that when considering the meaning of "person acting in an official capacity" (for the purposes of torture contrary s134(1) Criminal Justice Act 1988), there was a distinction between a military leader and a military governor, paras 65, 78. In the view of the majority, see para 79, whether an individual had a sufficient degree of organisation and control over an area, and exercised governmental functions, was a matter of fact and degree.
[76] Section 31(3).
[77] See section 31(5).
[78] Section 32(1)(e), (2). Provision is made to exclude a political party, such as Sinn Fein, that may be a governing party in the Republic of Ireland but is also a registered UK party: section 32(3).
[79] Particular reference was made in the government's Consultation Response on Hostile State Activity (12.7.22) of the need to avoid including "foreign-owned media groups". The position is different for foreign-owned companies for the purposes of Part 4 (Foreign Influence Registration Scheme) to which Schedule 13 applies.

The Two Modes

2.22. Crudely put, there are two ways of satisfying the foreign power: tasked and untasked[80].

Tasked: Conduct carried out for or on behalf of a foreign power

2.23. The formulation, "carried out for or on behalf of a foreign power", is wider than it might first appear.

2.24. This includes conduct instigated by, or carried out under the direction or control, of a foreign power[81] but also conduct carried out with financial or other assistance provided by a foreign power "for that purpose"[82], and conduct carried out "in collaboration with, or with the agreement of, a foreign power"[83].

2.25. "Financial or other assistance" might bring into scope any number of foreign-funded individuals and organisations. As pointed out in Parliamentary debate, certain well-known non-governmental organisations (NGOs) operating in the UK receive funding from foreign governments[84]. Foreign governments may provide other forms of assistances to NGOs, such as venues for conferences or information.

2.26. The government's answer in debate was that satisfying the Foreign Power Condition was not in itself wrongful and that more would be required to

[80] Although both modes may be present in any one case. This was true in the case of Daniel Khalife, prosecuted under earlier legislation. He both offered to spy for Iran, and was (later on) tasked by Iran: see Cheema-Grubb J., Woolwich Crown Court, sentencing remarks (25.1.25).
[81] Section 31(1)(a),(b).
[82] Section 31(1)(c).
[83] Section 31(2)(d).
[84] Hansard (HC) Vol 715 Col 616 (6.6.22). The qualifier "for that purpose" may rule out conduct that was never contemplated by the funder, but lobbying or public relations work is at the core of NGO activity and therefore deliberately funded.

commit an offence[85]. This is true, but some of the offences to which the Foreign Power Condition applies only require minimal conduct to amount to an offence. It is also true that foreign intelligence officers or agents may use NGO cover but there are separate offences to deal with this type of conduct to which the Foreign Power Condition does not apply[86].

- This illustrates the dilemma at the heart of the Act – how to tackle conduct that however well-meaning it appears, has a sinister purpose, without inculcating needless suspicion or paranoia about acts of generosity or friendship on the part of foreign governments.

2.27. **"**Collaboration" connotes active joint involvement, but "with agreement" might suggest both active and passive consent, for example where the activities of a Russia-based hacking collective are tolerated by the authorities on the basis that their activities are directed against Russia's enemies, providing a disruptive but deniable dividend[87]. But this would be to push the statutory language too far: mere tolerance is not the same as agreement, although in practice tolerance may sometimes demonstrate that some sort of agreement has been reached. No particular formalities are required for an agreement.

2.28. The relationship between the conduct and the foreign power may be direct or indirect. Section 31(3) expressly refers to "…an indirect relationship [with the foreign power] through one or more companies."[88].

---

[85] Hansard (HL) Vol 826 Col 1478 (11.1.23), Lord Sharpe of Epsom. The government has also asserted that conduct carried out on behalf of a foreign power will not involve the exercise of individual human rights (HM Government, Human Rights Memorandum to the NSA, at para 8) although this is strongly debatable given the extended meaning of "on behalf of".
[86] Sections 3, 17 (Foreign Intelligence Service offences).
[87] See Joint Committee on the National Security Strategy, 'A hostage to fortune: ransomware and UK national security', HC 194/ HL Paper 23 (13.12.23) at para 117.
[88] Section 31(3).

2.29. This aspect mitigates the exclusion of foreign-owned companies from the list of foreign powers because foreign powers may well act or communicate their wishes through companies that they control[89]. Whether a foreign company is acting as a puppet may be a nice question of fact and could in principle colour perceptions of working for a foreign university or publishing house[90].

2.30. Finally, the individual must "know, or having regard to other matters known to them ought reasonably to know", that the conduct is being carried out for or on behalf of a foreign power[91].

Untasked: Conduct intended to benefit a foreign power

2.31. The foreign power condition is also satisfied by conduct which is *intended to benefit* a foreign power, whether or not the foreign power is aware of it[92]. This might be termed the non-contact Foreign Power Condition.

2.32. This category is certainly aimed at corrupt or disillusioned United Kingdom officials who plan to sell secrets to the highest bidder without any external tasking from competitor States[93], but applies to any private citizen who volunteers to help. It is enough that they intend to benefit any foreign power, at some stage in the future, and it is not necessary for the prosecution to identify a particular foreign power which was intended to be benefited[94]. The same would apply to opportunistic hackers.

[89] State-owned companies may also provide cover for foreign intelligence officers or agents.
[90] Kendall, S., 'Espionage Law in the UK and Australia: Balancing Effectiveness and Appropriateness', Cambridge Law Journal, 83(1), March 2024, pp.62-98.
[91] Section 31(1)(b).
[92] Section 31(5). (Explanatory Notes, par 298).
[93] For example, the case of submariner Edward Devenney, who contacted the Russian embassy with secrets to sell: BBC News, 'Navy submariner jailed for Official Secrets Act breach' (12.12.12).
[94] Section 31(6) and Explanatory Notes, para 298.

2.33. Foreign “patriots” are brought into scope. In 2024 US intelligence agencies referred to individuals not under the direct supervision of the Chinese Communist Party who “may attempt election influence activities they perceive are in line with Beijing’s goals”[95]. The point is that some individuals act on their own initiative and do not need to be tasked.

2.34. The meaning of benefit is unqualified and there is no requirement of intending to benefit in a strategic or long-term sense. It seems that small acts may suffice, such as intimidating a single dissident.

2.35. The non-contact Foreign Power Condition is also calculated to alleviate problems of proof. Attribution, or proving that a particular state was involved in covert tasking is difficult at the best of times. It is even harder if the suspected state is more chaotic than command-and-control, corrupt, or willing to tolerate freewheeling “patriotic” ventures. Plus, a “false flag” operation may have been involved, where the defendant believes he is benefiting X state when in fact, unbeknown to him, he is assisting Y state.

2.36. Satisfying the non-contact Foreign Power Condition is no sign of illegality. It is but one element of certain offences under the NSA, and it is worth emphasizing that ordinary lawful conduct may well involve advancing the interests of other states within the international pecking order.

- Journalists, politicians and private individuals may argue passionately in favour of arming Ukraine in its war against Russia or returning the Elgin Marbles.
- Businesspeople promote trade deals with selected nations, for the mutual benefit of the UK and those other countries.

[95] Office of the Director of National Intelligence, ‘Annual Threat Assessment’ (5.2.24) at page 12.

- Charities lobby for financial support to needy populations, to the benefit of governments whose burden of care is lessened.
- Dual nationals and emigres often retain strong ties to a Foreign Power whose interests they may want to promote in exercise of their rights of free speech and association.
- However, sonorous statutory phrases like Foreign Power Condition can foster misapprehension. It is foreseeable that the government may need to do more to reassure individuals and organisations as the National Security Act 2023 becomes more widely known.

2.37. It would not be feasible, I think, to reform the application of the non-contact Foreign Power Condition so it only applied to the most serious State Threat offences: for example, to grievous bodily harm against a dissident but not online foreign interference. This would exclude prosecuting an influencer who set up a foreign interference shop for the highest state bidder. But the case for a non-contact Foreign Power Condition is evidently stronger in some cases than in others.

Course of Conduct

2.38. In all these cases the foreign power condition applies where the conduct "forms part" of a course of conduct that is carried out for or on behalf of a foreign power[96] either by that person or that person with others[97].

- The apparent purpose of the "course of conduct" provision is to ensure that defendants are liable for their role in collective or longer-term actions on behalf of foreign powers where individual components are

[96] Section 31(1)(a).
[97] Section 31(4).

left to individual discretion rather than being the subject of detailed tasking[98].

FPC as Aggravating Factor

2.39. Although sections 19 to 22 do not create new offences, they allow heavier sentences for non-National Security Act offences. If the foreign power condition is determined to be met on the evidence by the judge, the offence must be treated as aggravated.

2.40. From a prosecutor's perspective, aggravation is declaratory and deterrent. It is a means of signalling to foreign powers that their ruses have been uncovered, and to other individuals that they are at risk of detection. From the point of view of the individual, their act of theft or grievous bodily harm is treated as a matter of national security, meaning a heavier penalty and greater stigma.

2.41. Aggravation applies in each of the parts of the United Kingdom, and for services offices committed by armed forces personnel. For Scotland, the requirement of corroboration is disapplied for the purpose of proving the foreign power condition[99], reflecting the difficulties of proof when prosecuting espionage and the like.

[98] See Explanatory Notes, para 293.
[99] Section 21(4).

Prejudicial to the safety or interests of the United Kingdom

2.42. Prejudice to the safety or interests of the UK as a *purpose* is a component of 4 offences[100]; and as an *outcome* is material to 2 further offences[101].

2.43. This hallowed type of prejudice is undefined but, as indicated in Explanatory Notes[102], the government's intention was to bank previous caselaw on its meaning. The key legal authority concerned attempts to ground US warplanes taking off from Wethersfield Base in Essex in 1964. In summary, the House of Lords held that the safety and interests of the UK meant the objects of state policy determined by the Crown on the advice of Ministers[103]. It excluded the views of activists that the safety and interests of the UK were best served by a nuclear-free Britain.

2.44. The objects of modern state policy range far more widely than defence. Nothing is expressly excluded from the range of "safety and interests" and so these objects will certainly include:

- Protecting critical national infrastructure such as power generators or undersea cables.
- The healthy functioning of Parliamentary democracy.
- Economic macro-objectives such as achieving a lower rate of inflation or securing new trading arrangements post-EU Exit.

[100] The protected information offence (section 1), the offence of entering a prohibited place (section 4) and the sabotage offence (section 12); and where these are being prepared for, section 18 (acts preparatory).
[101] Assisting a foreign intelligence service offence in relation to activities conducted outside the UK (section 3) and engaging in foreign intereference (section 13) by creating an interference effect under section 14(1)(f).
[102] Paras 41-3, 69.
[103] Referring to Chandler v Director of Public Prosecutions (1964) AC 763 interpreting this phrase within the Official Secrets Act 1911.

2.45. There is plenty of scope for argument here. It may an object of state policy that the UK secures multiple golds at the Los Angeles Olympics in 2028, but sporting success was probably not contemplated as falling within the "safety and interests" protected by the National Security Act 2023. It could be said however the securing hosting rights to a future Football World Cup could have such important effect on the UK's economy, infrastructure, and international heft, as to fall the other side of the line.

2.46. The premise of the 2023 Act is more interconnected world[104], where computer or supply chain failure or theft of industrial secrets are all capable of bearing upon the UK's national security. As the editors of the leading textbook observe, in the national security context the distinction between promoting and protecting economic interests may have little if any practical significance[105]. But that comes with a danger of seeing competition between countries as a zero-sum game where a foreign company choosing not to build a car battery factory in another country is inevitably seen as prejudicial to the safety or interests of the UK, and vice-versa.

2.47. On economic interests, it would have been possible to adopt the drafting found in Schedule 3 to the Counter-Terrorism and Border Security Act 2019[106]. Threats to the economic well-being of the UK are included in hostile state activity but only if "in a way relevant to the interests of national security"[107]. Although "national security" can be criticised for vagueness, at least it offers a sense of proportion or gravity when considering economic threats.

2.48. By eschewing further definition, these are issues that courts will have to determine. It could be said that approaching the matter from the perspective of a 60-year-old case on military airfields provides insufficient guidance for

[104] Explanatory Notes, para 4.
[105] Ward, R., Jones, R., 'National Security: Law, Procedure and Practice' (Oxford, 2021), at para 3.16.
[106] See Chapter 6.
[107] Para 1(6)(b).

where the boundary lies between innocent or less culpable conduct, and conduct attracting the opprobrium and penalties of investigation and prosecution under the Act.

2.49. Moreover, exposure of embarrassing secrets is rarely if at all consonant with government interests, could impact the safety and interests of the United Kingdom (for example, by torpedoing sensitive trade negotiations), and could be part of malign state activity[108]. But it is the function of journalists to shine a light on chicanery by governments, office-holders, elected officials, and favoured businessmen, meaning that the fullest scrutiny must be brought on any attempt to use the NSA with respect to journalistic behaviour.

2.50. Prosecuting in cases of definitional uncertainty could taint and chill important manifestations of personal and collective freedoms such as a free press, the right to protest, securing an edge over economic competitors, and academic research[109]. This means that police and prosecutors will need to scrutinise with care the assessments they reasonably rely on from Ministers and officials, that particular conduct does in fact prejudice the safety and interests of the UK in a way that should lead to investigative action or prosecution.

2.51. On the other hand, the effect of earlier caselaw has been softened because, for most offences, the defendant must "know, or having regard to other matters known to them ought reasonably to know" that their conduct is prejudicial[110]. This is a welcome change, championed by the Law

[108] For example, a hack-and-leak operation against government databases.
[109] Noting Professor Sir David Omand's warning about shroud-waving: "…just because agile minds can conceive of chilling does not mean that it should necessarily have significant weight in the balance" Examining the Ethics of Spying: A Practitioner's View' in 'National Security Intelligence Activity and the Just Intelligence Theory' Criminal Law and Philosophy (2024) 18:805–818.
[110] Section 1(1)(b) (espionage); section 4(1)(b); section 12(1)(c).

Commission[111], because otherwise a person could be convicted where they were oblivious to the wider ramifications of their actions.

Know or ought reasonably to know

2.52. The mental element, "know, or having regard to other matters known to them ought reasonably to know" appears throughout the NSA and is likely to be the main issue in criminal proceedings. I refer to it as actual or constructive knowledge.

- It is a component of the Foreign Power Condition (section 31) and thereby relevant to all those offences which depend on its satisfaction[112].
- It is a discrete requirement in relation to six offences[113].

2.53. Actual or constructive knowledge is not intent or motive, and the NSA applies to people who assist foreign powers for mercenary as well as ideological reasons. It is not the same as belief; indeed, belief would allow defendants to argue the toss about whether they truly believed, for example, that the UK would be better if official secrets were shared abroad[114]. Suspicion is not enough.

2.54. Courts have not generally found it necessary to direct juries about the meaning of actual knowledge[115]. Conventionally, it has been interpreted as including wilful blindness, such as shutting one's eyes to an obvious means of knowledge or deliberately refraining from making enquiries the result of which

[111] Law Commission Report, supra, at para 3.47 et seq.
[112] Sections 1, 2, 12, 13, 16, 19-22 and in part, 18.
[113] Sections 1, 2, 3, 4, 5, 12 and 17.
[114] Law Commission, Protection of Official Data, A Consultation Paper (no.230, 2018), at 2.28 citing J C Smith and B Hogan, Criminal Law (6th ed, 1988) pp 840-841.
[115] If further assistance is required a jury might be told that D knew X if D was sure of X: Crown Court Compendium (June 2023) Vol 1, 8-17 at para 24(1)).

the person does not care to have, although the boundaries of wilful blindness are imprecise[116].

2.55. As to constructive knowledge, the formulation "having regard to other matters known to them ought reasonably to know" is rare, but not unknown[117]. It imports an element of objectivity ("ought to know") which is not necessarily present in actual knowledge (including wilful blindness). It therefore appears that a person is to be judged according to what a reasonable man would know having regard to all the other matters known to that person.

2.56. The difficulty is that foreign powers are crafty, will mask their involvement by use of proxies or cut-outs and may target dupes. For example:

- A person who is asked by foreign business contact to secure binoculars for birdwatching near a military airfield may simply not put two and two together. Ought he to know that he is being tasked by foreign power, just because he does not realise what other people would?
- A person who is asked discretely to find a flat for an embassy official may not realise, even if a reasonable person would, that ordinary diplomats have other ways of securing accommodation and that the request was a red flag for covert activity. Ought such a person "reasonably to know" that they are materially assisting a foreign intelligence service[118] in securing a safehouse?

[116] See the discussion in Smith & Hogan, supra, at 5.2.7. They cite Lord Devlin's distinction between (i) actual knowledge (ii) wilful blindness (knowledge in the second degree); (iii) constructive knowledge (knowledge in the third degree). Constructive knowledge is therefore distinct from wilful blindness.
[117] It plays a role in the common law offence of manslaughter, where D has created or contributed to the creation of a state of affairs which he knows, or ought reasonably to know, has become life threatening, and incurs a duty to act by taking reasonable steps to save another's life (R v Evans [2009] EWCA Crim 650, para.31). It is an aspect of the jury research offence under section 20A Juries Act 1974.
[118] Section 3.

2.57. The offence could therefore drag up the naïve or ill-informed. Given the nature of the offences and their potential penalties, interpreting "ought reasonably to know" against a purely objective standard invites unjust outcomes. A person who is inveigled into an apparently innocent favour or business deal is not in an analogous position to a person who chooses to drive a car on a public road according to objective safety requirements, or who handles a gun without checking whether it is loaded[119], where higher standards of behaviour can be expected.

2.58. Parliament was undoubtedly aware of the risk to innocent dupes during the passage of the Bill. In the House of Lords, a government-sponsored amendment was passed that added the words "having regard to other matters known to them" to the words "ought reasonably to know". This was said to clarify that those who engaged in conduct "unwittingly – who did not know but are told that they should have known" would not be caught, and thereby avoid "imputed knowledge"[120].

2.59. In documentation accompanying the Bill, the government even stated that turning a blind eye knowledge was an example of where a person "ought reasonably to know"[121]. In other documentation the government stated that a person would not be caught if they acted "unwittingly"[122].

2.60. But whatever the government's expressed intention, it is difficult to interpret the word "reasonably" without importing some element of objectivity meaning that individuals can be prosecuted for what they should have known, and not only what they actually knew[123]. Once the precise circumstances known to the defendant are taken into account, his or her naivety appears to

[119] Cf. S [2015] EWCA Crim 558.
[120] Hansard (HL) vol 828, col 249 (1.3.23), Lord Sharpe of Epsom.
[121] Human Rights Memorandum (2023) at para 26, with reference to the section 3 offence.
[122] HM Government, Policy Paper, 'Journalistic freedoms: National Security Bill factsheet (updated 19.8.24).
[123] Cf reasonable cause to suspect, where Lane and Letts [2018] UKSC 36 were liable to be convicted, whether or not they knew or suspected their money transfers were funding terrorism.

be a matter that merely goes to the public interest in prosecution or length of sentence[124].

2.61. In practice, I suspect that prosecutorial discretion, including prosecutors' assessments of likely jury reaction, will have an important role in determining whether cases of naïve dupes reach the courts in the first place.

2.62. But this is something I intend to keep under review because of the risk of unjust outcomes. Depending on how the legislation operates in practice, it may be necessary to consider omitting the word "reasonably" or to provide a statutory defence that the defendant did not in fact suspect the matter of which he is accused.

[124] There is the useful discussion on this topic by the Final Hong Kong Appeal Court in Hksar v Murlidhar [2019] HKCFA 47.

3. OFFENCES

3.1. Some of the National Security Act 2023 offences are reimagined from earlier legislation with new technology uppermost. These are the offences concerning protected information, prohibited places and preparatory conduct. Others are wholly new types of criminal liability, directed at trade secrets, foreign intelligence services, sabotage and foreign interference. The overall effect is an overlapping mosaic of criminal liability, where any given conduct will often amount to more than one offence.

Information Offences

Obtaining or disclosing protected information (Section 1)

3.2. Section 1 is classic spying, updated for the modern era, and carries a maximum penalty of life imprisonment.

3.3. The currency of this offence is "**protected information**", given a full-bore definition of any information, document or article[125], including information about tactics, techniques and procedures[126], where either:

- access is restricted "in any way" for the purposes of protecting the safety or interests of the United Kingdom[127]; or
- access would reasonably be expected to be restricted[128].

3.4. Formalities are not important. Whilst it will obviously apply to official marked information (TOP SECRET, SECRET and OFFICIAL), no government marking

[125] For article, the Explanatory Notes, para 71, give as examples a prototype, model or memory stick.
[126] See section 34(1).
[127] Section 1(2)(a).
[128] Section 1(2)(b).

need be applied to the information, document or article if access is restricted in any way (for example, by a locked door or using password protection) for the purposes of protecting UK safety or interests.

3.5. The information, document or article does not have to be held at a government location or by a government official, and the restriction can be applied by anyone. This draws in a potentially wide pool of people outside government and the police whose conduct, and belief about the nature of the information, may determine whether the offence applies.

- If a barrister prosecuting a sensitive espionage trial locked her handwritten notes away in a safe at home, that would count as a restriction for the purposes of protecting the safety or interests of the UK.
- If a newspaper collated details of sensitive intelligence techniques and protected the information in safe because aware that could compromise national security, the offence would apply if the information was stolen by foreign spy, even though the document never seen by authorities.
- The restriction could be applied by a scientist working on a process with military application. At first glance, it would seem to apply even if the scientist *overestimated* the significance of his information to UK safety or interests, when it was merely a trade secret (to which section 2 would apply). I would however expect prosecutions only where there was an element of objective risk to UK safety or interests.

3.6. It applies where access has not been restricted, by negligence or for more sinister purpose, where restriction would be reasonably expected[129]. It continues to apply after the protected information, for example the names of police officers who work with UK intelligence agencies, has been leaked or stolen.

[129] Section 1(2)(b).

- The next recipient, for example a journalist, may be unaware of its provenance but would be in possession of protected information if it was reasonable to expect access to be restricted by looking at the information.
- This places a burden on the recipient to determine whether the information should have been protected even if it has no protective marking[130].
- It also raises the issue of the point or threshold at which the safety or interests of the UK become relevant. Unearthing facts and exposing wrongdoing will become a practical impossibility if journalists cannot deal with information on the off-chance that the authorities will subsequently say that it ought to have been protected for national security reasons.
- For example, a Chief Whip might lock away written information about an MP's misbehaviour in part on the basis that its disclosure would open the MP to blackmail by foreign powers. A junior whip then leaks this information to the press who approach the Chief Whip with the information.
- It would be objectionable if the press were threatened on the basis that they were dealing with protected information to which section 1 applied. Journalists will have to stand firm and be prepared to call the bluff of those who overclaim.

3.7. The **conduct element** of spying is obtaining, copying, recording, or retaining the protected information, or disclosing or providing access to it[131].

- The concept of "providing access" is potentially overbroad.

[130] As the National Union of Journalists and others pointed out in evidence during the passage of the Bill.
[131] Section 1(1)(a). Retaining and disclosing are further defined in s1(5)(b).

- A spy who tells his colleague where he has hidden the stolen information arguably provides access to it. It could even be argued that a support agent who tells a spy where a locked safe containing secrets is to be found provides access to the secrets, even though a further stage (safe-breaking) is required[132].

3.8. The conduct can take place anywhere in the world[133], and the offence can be committed by non-nationals as well as nationals[134]. In the cyberespionage era, it is hard to imagine any narrower jurisdictional remit.

3.9. **Two further elements**, each comprising requirements of actual or constructive knowledge, must also be satisfied.

3.10. Firstly, although the defendant does not need to know or suspect that the information is protected, their person's conduct must be for a purpose which they know (or reasonably ought to know) is prejudicial to the safety or interests of the UK[135].

3.11. In effect, a person who obtains information with the forbidden purpose has to live with the risk that the information is protected information. In practice the spy will often be overcoming physical (safes) or electronic (passwords) hurdles of some description, so the existence of a restriction will be well understood by them.

3.12. Secondly, the foreign power condition must be met[136].

---

[132] The example of providing access given in the Explanatory Notes, para 82 (albeit in relation to trade secrets) is disclosing access codes, which allow remote access to information.
[133] Section 1(3).
[134] Section 36(1), thus increasing the ambit of this offence compared to its statutory predecessors in the 1911 and 1920 Acts.
[135] Section 1(1)(b). Under section 1 of the Official Secrets Act 1911, the defendant did not have to know that his purpose was prejudicial.
[136] Section 1(1)(c).

3.13. It follows that the focus offence is not the utility of the stolen information to that foreign power[137] but the purpose prejudicial to the UK, coupled with acting for a foreign power. So, a person who, intending to benefit Country A, steals an OFFICIAL document from a locked safe in a government building commits an offence even if the document is useless to the foreign power – it seems to be enough that he knows his purpose, taking marked documents from a government safe, is prejudicial to the safety and interests of the UK.

3.14. When the defendant is an insider, the foreign power condition is the key difference between this offence and the offences under the Official Secrets Act 1989. The conduct of leaky government officials falls under both Acts, but it only amounts to a spying offence (max life imprisonment) as opposed to a disclosure offence (max 2 years) if done for a foreign power.

3.15. There is no public interest whistle-blowing defence, and the government's desire to avoid this thorny issue explains why the Official Secrets Act 1989 was not incorporated into or reformed by the NSA[138].

Obtaining or disclosing trade secrets (Section 2)

3.16. This is a wholly new offence, responding to long-articulated fears about foreign powers, above all China, securing long-term economic advantage through extracting valuable trade secrets by subterfuge[139]. It reflects the government's view that the distinction between economic and national security has become increasingly redundant[140].

3.17. This type of activity was identified by the government as inherently harmful, and the striking effect is that for this offence, the prosecution does not

[137] Contrast section 1 of the 1911 Act.
[138] Hansard HC Deb, vol 715, col 571, 6 June 2022 (Home Secretary).
[139] See for example, Intelligence and Security Committee, China Report, HC 1605 (13.7.23).
[140] Ingrated Review of Security, Defence, Development and Foreign Policy (16.3.21).

need to prove prejudice to UK safety or interests[141]. This is reflected in the lower 14 year maximum.

3.18. To be a "**trade secret**" the information document or other article must satisfy three criteria[142]:

- It must not be "generally" known by or available to persons with knowledge or expertise in the field. It should be noted that since the end of the Cold War and the dominance of the internet, huge amounts of information relevant to national security have entered the public domain. Academics are hard-wired to cooperate and rely on open-access publications to gain professional success. This type of information is not the stuff of trade secrets.
- It must have not only actual or potential "industrial, economic or commercial value" but that value must be capable of being adversely affected if it became generally known in the field, since value is linked to secrecy[143].
- It could reasonably be expected to be subject to restrictive measures. At this point, it appears necessary to consider not just the information itself but the surrounding circumstances.

3.19. The intention appears to be to include "articles" from which trade secrets may be derived[144], presumably by analysis. If it concerns a secret prototype this is clear enough. But a sophisticated researcher could extract a trade secret from an article on general release (for example, the secret recipe for Coca Cola), knowing full well that the secret is valuable and held on a restricted basis.

---

[141] HM Government, Human Rights Memorandum, para 19.
[142] Section 2(2). The criteria are modelled on those in Regulation 2 of the Trade Secrets (Enforcement, etc.) Regulations 2018.
[143] Explanatory Notes, para 78. Scholars of English literature can breathe a sigh of relief.
[144] Explanatory Notes, para 79.

3.20. The conduct element includes the same actions as the section 1 offence (obtaining, copying, recording, or retaining the protected information, or disclosing or providing access) but it must be "**unauthorised**"[145]. This has a slightly complex meaning to cater for lone inventors do not require authorisation for sharing their trade secrets[146].

3.21. In the case of information derived from reverse-engineering the Coca Cola secret recipe, the conduct involved in obtaining or retaining the trade secret would not qualify as "unauthorised". Reverse engineering is generally considered a lawful way of acquiring trade secrets[147] and is the risk taken by a company which releases its products on the general market. A successful reverse engineer is then entitled to make whatever use he wants of the information. Any subsequent disclosure by that person could not count as "unauthorised".

3.22. There are two additional requirements for the offence, both involving some element of mental awareness.

3.23. Firstly, the individual must know actually or constructively (know, or having regard to other matters known to them ought reasonably to know) that their conduct is unauthorised[148].

3.24. Secondly, the foreign power condition must be met[149]. This is the only point at which the interests of national security intersect with what would

[145] Section 2(1)(a) and (b).
[146] Section 2(3).
[147] A person who undertakes the exercise of reverse engineering a publicly accessible article, rather than taking a short cut by misusing a confidential document, is free to use the information obtained as a result of that exercise even if it takes a significant amount of work: JC Bamford Excavators Ltd v Manitou UK Ltd [2023] EWCA Civ 840, at para 50.
[148] Section 2(1)(c).
[149] Section 2(1)(d).

otherwise relate purely to conduct affecting private interests. It is not necessary that the trade secret will assist with the foreign power's state activity (such as defence); it might be that the foreign power simply intends to make the secret available to local businesses.

3.25. A weaker form of extra-territorial jurisdiction applies than under section 1. Conduct that takes place wholly outside the UK may result in criminal liability only if the trade secret is in the possession or under the control of a UK person[150]. In essence, this refers to UK nationals or companies or other legal bodies formed under UK law, as well as those of whatever nationality who live in the UK[151].

3.26. So,

- A foreign national who is working for a foreign power commits an offence if she steals trade secrets from a London-based foreign company, if she is present in the UK.
- She also commits an offence if she carries out a computer hack from London into a Paris-based foreign company to steal trade secrets.
- However, if her conduct is performed wholly outside the UK, she only commits an offence if she obtains the trade secret from a UK person or company. That could be through hacking into a UK-based company from overseas or obtaining it from a UK scientist holidaying abroad.
- The offence also captures industrial spies and their targets whose presence in the UK is incidental, such as foreign businesspeople attending conferences.

[150] Section 2(4), (5).
[151] Section 2(6), (7). This is an example of passive personality jurisdiction. More ordinarily, see for example section 17(3A) Terrorism Act 2006, qualified extensions of extra-territorial jurisdiction are based on the nationality of the offender.

3.27. Although less than under section 1 (life), 14 years is a heavy maximum tariff for dealing with private information.

3.28. Since there is no additional requirement that the purpose of any unauthorised conduct is known to be prejudicial to the safety and security of the UK, the need to satisfy the foreign power condition is all that stands between unscrupulous economic rivals, or responsible journalists dealing with leaks and sources, and a prosecution under national security legislation. The acceptability of this offence is therefore highly dependent on the fair and effective operation of the Foreign Power Condition.

Foreign Intelligence Service offences (Sections 3 and 17)

3.29. Two new offences bring attention to the interactions, which may appear quite ordinary on the surface, between individuals and the intelligence systems of foreign powers, and are intended to fulfil the government's intention of criminalising being an undeclared intelligence officer in the UK[152].

3.30. In effect, they incorporate into UK criminal law a toxic zone around Foreign Intelligence Services (FIS). Other offences exist to penalise specific intelligence activities such as espionage – these offences have a different focus, by penalising a very broad range of interactions with persons having the status of FIS.

3.31. The offences are also the most difficult offences to pin down within the NSA, owing to the vagueness of the definition of Foreign Intelligence Service (FIS) and the fact that it applies both to friendly and hostile services. No Foreign Power Condition applies; nor is there any need to show a purpose prejudicial to the safety and interests of the United Kingdom.

[152] HM Government, Policy Paper, 'New espionage offences: factsheet' (19.8.24).

3.32. The FIS definition is lexically short but conceptually broad because there are no universal standards for organising the intelligence activities of foreign powers of concern to the United Kingdom. Drafted with the "whole-state" approach of certain foreign powers firmly in mind[153], the function-orientated definition discussed below is capable of capturing certain diplomats[154], police, foreign ministries, private companies[155], and student bodies tasked with reporting back to the mother country[156], as well as conventional intelligence bureaux.

- In their China report, the Intelligence and Security Committee referred to the sheer difficulty in pinning down the Chinese intelligence bodies. The nature and scale of their services were "hard to grasp" due to China's size, the blurring of lines of accountability, its partial decentralisation, and lack of information; plus, the Chinese Communist Party "…co-opts every state institution, company and citizen"[157].
- A FIS definition that only extended to traditional spy agencies would be far too limiting.

3.33. However, there are risks in labelling:

- Accusing foreign linked individuals or bodies of being vehicles for spying as a means of delegitimising them is a tactic for repressive states[158].

---

[153] HC (Public Bill Committee) (8.9.22), Security Minister.
[154] Cf. Ardavan M. Khoshnood & Arvin Khoshnood, The Islamic Republic of Iran's Use of Diplomats in Its Intelligence and Terrorist Operations against Dissidents: The Case of Assadollah Assadi (2024) 37 International Journal of Intelligence and CounterIntelligence 976.
[155] Explanatory Notes, para 90. Cf. Joshi, S., 'Private firms and open sources are giving spies a run for their money' (Economist Technology Quarterly, 1.7.24).
[156] Kulandtick, J., 'Beijing's Campus Offensive', Council for Foreign Relations (14.4.23).
[157] China report, supra, at Annex B, paras F-H.
[158] Or as "foreign agents"; see Kobaliya and Others v. Russia (application no. 39446/16, 22 October 2024), European Court of Human Rights; Cameron, J., and Nicola, F., 'The Spreading Impact of Restrictive 'Foreign Agent' Laws and How to Stop Them' (Just Security, 10 December 2024).

- Think tanks, charities, journalists, foreign citizens resident in the UK, and many others are bound to engage with emanations of foreign powers which may qualify as FIS[159].
- Excessive zeal about contact with FIS could require rethinking of innocent contact or lead to demands from oversight boards or regulators to the wider detriment of our open society and the rights and freedoms of individuals.
- The nomenclature "Foreign Intelligence Service" is perhaps regrettable, when what is clearly intended by the definition is a much broader category than shadowy spy agencies.
- It may be useful to view the definition of FIS as a starting point for the offences: whether a criminal investigation is mounted or a prosecution brought will depend much more on the nature of the interaction between the individual and the FIS[160].

3.34. By section 3(10), a FIS means:

> "…any person whose functions include carrying out intelligence activities for or on behalf of a foreign power"[161].

3.35. The use of the word "person" recognises that individuals may qualify as FIS, even though they operate within host structures that have little to do with intelligence matters[162]. Private as well as public bodies are included: the

[159] Especially given that the 11th Bureau of the Chinese Ministry of State Security, the Chinese Institute of Contemporary International Relations, is a respected think tank: Joske, A., 'Secrets and Spies: How China's Greatest Covert Operations Fooled the World' (Hardie Grant, 2022)..
[160] For example, if accredited staff from a foreign embassy provide a UK resident with a covert communication device, it is this conduct that will lead to investigation and prosecution.
[161] This definition is country neutral, applying as much to the FIS of the Five Eyes intelligence community (US, Australia, Canada, New Zealand) as it does to Russia's FSB or FRU. Under the Interpretation Act 1978 person includes a body of persons corporate or unincorporate.
[162] See Joske, A., 'Secrets and Spies: How China's Greatest Covert Operations Fooled the World' (Hardie Grant, 2022).

government expected the formulation to cover "a private contractor who is employed to provide security and intelligence services for a foreign power"[163].

3.36. There is no statutory definition of "intelligence activities"[164] [165] and it is no part of my role to attempt to supply one. They are not confined to covert activities, nor are they limited to intelligence concerning national security matters, or at least national security matters as they would be considered domestically[166].

3.37. There is no correspondence test which confines FIS to institutions playing similar roles to UK intelligence agencies such as MI5, but "intelligence activities" would seem to include *at a minimum* actions conventionally carried out by them: gathering of national security-relevant sensitive and open-source information (by agents, signals intelligence, imagery intelligence, geospatial intelligence, hacking, bugging, surveillance, bulk collection); counterintelligence; assessment of information to glean insights relevant to national security; liaison relationships; training in tradecraft; protective security; vetting; and certain military operations[167]. But not necessarily all[168].

---

[163] NSA Explanatory Notes para 90.

[164] Intelligence activities are repeatedly referred to in military doctrine, for example, Ministry of Defence, 'Intelligence, Counterintelligence and Security Support to Joint Operations. Joint Doctrine Publication 2-00' (4th edition, 2023), but not defined.

[165] I am grateful to Dr Ewan Smith of University College London for his analysis of the meaning of "intelligence activities".

[166] For example, if the Chinese MSS intelligence agency decided to gather information on UK cats and dogs, this would seem to count as "intelligence activity" even though outside the remit of the UK intelligence agencies.

[167] See Explanatory Notes to Justice and Security Act 2013, paragraph 127, referring to intelligence activities carried out by the Special Forces. It is an interesting question whether intelligence activities include coordination and oversight of those activities. In a United Kingdom context this would include for example the Home and Foreign Secretaries, their ministerial deputies, the Intelligence and Security Committee of Parliament, and the Investigatory Powers Commissioner. There is nothing in the definition to discourage such a wide reading of the definition.

[168] Under the Intelligence Services Act 1994, section 3(1)(b), one of GCHQ's functions is to provide language assistance to government.

3.38. "Function" implies more than incidental or ad hoc involvement – in other words, a person does not become a FIS merely because they become involved in intelligence activities[169]. However, the carrying out intelligence activities need not be the person's predominant function. The question of whether a person has a "function" of carrying out "intelligence activities" will be a matter of fact. No doubt a person's conduct may well reveal that they have that function, for example the use of spy tradecraft.

3.39. The difficulties with the definition are twofold. Firstly, once a person has the status of FIS, then it applies even though much of their day-to-day conduct has nothing to do with intelligence activities. Once a FIS, always a FIS until the person's function changes. Secondly, "intelligence activities" can appear very different depending on who is carrying them out. Local police forces might out carry out test-purchase operations in supermarkets – these are intelligence activities. Some police forces (like the Metropolitan Police in the UK) may carry out intelligence activities on behalf of the government – they will qualify as FIS too.

3.40. Part of any foreign ambassador's function is to gather information and generate insights on behalf of and in the interests of a foreign power[170]. No doubt that will include information provided on the host country's military and security posture. But Parliament cannot have intended to label ordinary diplomats, operating openly and under the protection of the Vienna Convention, as FIS. Undeclared intelligence officers acting under diplomatic cover are another matter.

---

[169] In this context, function appears to imply having a task (carrying out intelligence activities) rather than having an objective (contrast, the Security Service Act 1989, section 1, under which MI5's functions are to protect national security, in the sense of having a goal or objective).

[170] Cf Article 3 Vienna Convention on Diplomatic Relations (1961). In 'Espionage, Secrecy, and Institutional Moral Reasoning', Criminal Law and Philosophy (2024) 18:819–832, Ratner, S., refers to the routine work of diplomats posted abroad, sifting through public sources like policy papers and records of public inquiries, as a form of intelligence collection.

3.41. It will be a question of fact whether the intelligence activities are "for or on behalf of a foreign power". The definition excludes those who are merely intending to benefit a foreign power through their activities. For example, a private hacking collective which aims to gather information with a view to selling it to a foreign power at a later stage is not a FIS[171]. In next year's report I will consider the implications of the existence and use of proxies willing to carry out intelligence activities.

Assisting a Foreign Intelligence Service (Section 3)

3.42. There are two ways of committing the section 3 offence which carries a maximum of 14 years' imprisonment.

The Intentional Offence

3.43. This comprises an unlimited conduct element ("conduct of any kind") together with the highest mental element, intent. A defendant must intend his conduct "to materially assist a foreign intelligence service in carrying out UK-related activities" [172]. The intent element operates as a form of penal alchemy to transform the conduct (base metal) into crime (gold). The model is familiar from attack-planning contrary to section 5 Terrorism Act 2006.

3.44. The ways of **materially assisting** intelligence goals are manifold[173]. Preparatory steps may appear innocuous at face value. For example, assistance may be rendered by making an introduction to a friend at a party, because it may assist in later recruitment as an agent or co-optee[174]; renting a house, which is in fact a safehouse; setting up a company, actually a shell

[171] Contrast the Foreign Power Condition which includes activity intended to benefit a foreign power.
[172] Section 3(1).
[173] A compendious survey of Russian techniques is in Riehle, K., 'Russian Intelligence: A Case-based Study of Russian Services and Missions Past and Present' (National Intelligence Press, 2022).
[174] A co-optee is someone whose legitimate contacts, profile or business activities may allow access to individuals of intelligence interest: see Annex C of the Schedule 3 Code of Practice (Home Office, January 2024).

company to provide funds to another company which is a cover for a FIS[175]; gathering open source information, as later analysis may help to identify the movements of military personnel[176].

3.45. But it will be noted that the intention can relate to any **UK-related activities** of a FIS, not just UK-related *intelligence* activities[177]. For defendants within the UK, UK-related activities are simply "activities taking place in the United Kingdom" and need not be damaging to national security[178].

- It is not immediately clear what the word "materially" adds, but assuming it means "more than trivially", then this offence could be committed by an UK-based embassy cleaner or cook.
- A more satisfactory gloss on the meaning of the phrase might put greater emphasis on assisting the *work* of the FIS: a cleaner or cook, however essential to the day-to-day functioning of a FIS, would not be said to assist in the *work* of the FIS[179].
- But this is a thin boundary: providing banking services might materially assist the work of a FIS even if in connection with overt activities, such as writing a publication on threat levels for a foreign audience.
- Nor would this gloss exclude the FIS's personal secretary, or an individual who introduces an overseas liaison police officer to an academic or government contact.
- The fundamental difficulty with the offence – readily explicable by a desire to catch the widest range of assistance to malign intelligence activities – is that it is based on the status of the FIS rather than the

[175] See Explanatory Notes, para 84, Example 2.
[176] Van Puyvelde, D., Tabárez Rienzi, F., 'The rise of open-source intelligence. European Journal of International Security'. Published online 2025:1-15.
[177] For UK-based defendants
[178] Section 3(4)(a). Other parts of the NSA, such as the espionage offences (sections 1 and 2), are available for those who are recruited to carry out the more obvious harmful tasks.
[179] I am grateful to Professor David Omerod KC for his suggested jury direction that "materially" simply means that the assistance would have been such as to "make a difference" to the work of the FIS.

status of the services rendered. The greatest care is required in how this offence is deployed.

3.46. The position is different where assistance is to **"UK-related activities" taking place outside the UK**. External activities only count if they are prejudicial to the safety or interests of the United Kingdom to attract liability[180]. Otherwise, for example, a French citizen who assisted a FIS to design their Paris headquarters would commit an offence under UK law.

3.47. This begs the question of whether FIS activities abroad against UK *allies* are inherently prejudicial to UK interests. There are various ways in which using the UK as a base for carrying out intelligence activities against allies could be directly or indirectly prejudicial. Compromising one of the other Five Eyes intelligence-sharing partners might have direct effects on UK security; indirect effects might arise from the risk of damage to mutual trust and cooperation should that ally ever find out that the UK had been used as a base.

3.48. A person may commit the offence for their conduct committed partly in the UK and partly abroad, but considerations of comity – a recognition that other countries are just as entitled to have spy agencies as the UK – limits offences concerned with Foreign Intelligence Services to conduct wholly abroad by UK persons or Crown employees[181].

- This amounts to a worldwide ban on assisting FIS in UK-related activities for UK nationals, UK companies and individuals of whatever nationality who "live in" the UK[182].

[180] Section 3(4)(b).
[181] Section 37(2) referring to sections 3(6) and 17(6). "Crown employees" ensures that non-nationals working for British embassies abroad are within scope: Explanatory Notes, para 86.
[182] Section 3(10) applying the definition in section 2(6). This is subject to the "arrangements" defence considered below.

- Anyone else can assist a FIS if their conduct is wholly outside the UK, although remote hacking of UK systems[183] might count as partly in the UK[184].

3.49. It is not necessary to **identify** a particular FIS when proving an offence[185]. This caters for "false flag" operations (where a person intends to assist service A which is being impersonated by service B), or cases of assistance-offering (where a defendant is willing to sell their services to any FIS and is shopping around for a buyer[186]).

The Likely Assistance Offence

3.50. Secondly, a person commits an offence if he engages in conduct that is "likely to materially assist" a foreign intelligence service in its UK-related activities, where he knows actually or constructively ("knows, or having regard to other matters known to them ought reasonably to know") that his conduct has that effect[187].

3.51. Section 3 specifies that providing, or providing access to information, goods, services or financial benefits whether directly or indirectly "may" be likely to have that effect – whether it is in fact likely to have that effect will depend on the precise circumstances.

---

[183] The internet makes it entirely possible for domestic intelligence officers to carry out intelligence operations on foreign soil without setting foot there. See for example, US Department of Justice indictment against Iran-based IRGC operative, Shahram Poursavi, Case: 1:22-mj0-176 (August 2022), regarding a plot to assassinate former National Security Advisor John Bolton on US soil.
[184] Although, by analogy with the Supreme Court's extradition in decision in El-Khouri v Government of the United States of America [2025] UKSC 3, a distinction is to be drawn between conduct "in" a country, and the different question of whether UK courts would have jurisdiction based on the intended or felt consequences of the conduct (see para 58). If it related to protected information, such a person would in any event commit the section 1 offence.
[185] Section 3(5).
[186] Explanatory Notes, para 85.
[187] Section 3(2).

3.52. As introduced in the original Bill, the formulation was looser ("conduct of a kind that it is reasonably possible may materially assist…"[188]). The current wording is an improvement, but its origins show that the intention of this offence is to focus on the capability of conduct to assist rather than any assistance concretely rendered[189]. It will cover those who have no intention to assist a foreign intelligence but know (actually or constructively) that their conduct is likely to do so. There is no requirement for any contact, direct or indirect, with a FIS

3.53. Whilst unobjectionable where the individual has some conscious and direct dealings with a foreign power, and deliberately engages in conduct which is likely to assist them in traditional spying, it also could apply to those whose potential assistance is more remote, for example:

- An artificial intelligence researcher who puts his novel code on a public-access platform[190], believing strongly in the importance of open collaboration, where this code is likely to assist a FIS in hacking UK-based computers.
- A committed anti-vaxxer or climate activist, who reasonably ought to know that his social media or protest activity is likely to assist a FIS in fostering divisions within UK society.

3.54. What stands between these examples and real-world consequences is how police, prosecutors, and courts interpret the word "material" and the word "likely"; and how the authorities exercise their discretion in practice.

3.55. When the courts were confronted with a broadly analogous provision under terrorism legislation (possession of information of a kind likely to be

[188] Clause 3(2).
[189] Cf. section 58 Terrorism Act 2000.
[190] Such as GitHub.

useful to a person committing or preparing an act of terrorism[191]), they concluded that the information in question had to be inherently useful[192], for example, an instructional bomb manual, but not the London A-Z.

3.56. It is quite possible that the courts will be called upon to carry out a similar exercise here. At present, this aspect of the section 3 offence appears overbroad because of the very wide nature of conduct that is likely to materially assist a FIS (noting its broad definition) in carrying out its UK-related activities[193]. This apparent overbreadth is aggravated by the lesser mental element based on constructive knowledge (reasonably ought to know) which is capable of sweeping up the naïve and ignorant.

3.57. One of the examples of the offence given in the Explanatory Notes[194] concerns a defendant who provides ask-no-questions company formation services to an acquaintance at a foreign embassy.

3.58. According to this example, the purpose of the shell company is to provide funds to another company which is acting as cover for a FIS. The Explanatory Notes state that based on everything the defendant knows about his embassy acquaintance, he "…ought reasonably to know that [his] conduct is likely to assist the foreign intelligence service in carrying out activities in the UK". This is complicated:

- It cannot be the case that any 'shady business' with an embassy contact is sufficient notice that such conduct is likely to assist a FIS: the embassy contact could have other venal reasons, such as financial corruption, for wanting a shell company.

[191] Section 58 Terrorism Act 2000.
[192] R v G [2009] UKHL 13.
[193] The position is less troubling where the UK-related activities of the FIS are outside the UK: in this case they must be prejudicial to the safety or interests of the UK (section 3(4)(b)).
[194] Second example at para 84.

- Nor is such notice going to come purely from knowledge of the status of the embassy acquaintance. As suggested earlier, the mere fact that an individual is accredited as a diplomat with involvement in the defence and security sphere (e.g. a defence attaché) does not make him a FIS.
- Notice must come from a combination of knowledge of the acquaintance, and what is being requested from the defendant, in the particular circumstances[195]..

3.59. I consider below whether the defences in section 3 are sufficient to protect the innocent.

Obtaining or agreeing to obtain material benefits from a foreign intelligence service (Section 17)

3.60. The subject matter of this offence is any "material benefit". Material benefits are defined as potentially including ("may include") financial benefits, anything which has the potential to result in a financial benefit[196], and information[197].

3.61. For an offence to be committed, the material benefit must have been provided by or on behalf of a foreign intelligence service (FIS) or be intended to be provided in future by a FIS[198]. The material benefit may be provided directly, or indirectly, for example through one or more companies[199],

[195] A more persuasive example is given HM Government policy paper 'New espionage offences: factsheet' (12.2.24) – in this example, the defendant suspects that his business contact at the UK embassy of Country A is an intelligence official, knows that Country A's intelligence service carries out hostile reconnaissance of dissidents in the UK, and nonetheless provides surveillance software on a cash/hush-hush basis. The third example in the Explanatory Notes is also clearer.
[196] Meaning money or money's worth: sections 3(10) and 17(12).
[197] Section 17(3).
[198] Section 17(1)(b), (2)(b).
[199] Section 17(5).

recognising the obfuscated layering likely to be employed by FIS in getting payments to agents.

3.62. There is no dispensation, as there is in section 3[200], that the prosecution does not need to identify a particular foreign intelligence service – it is not clear to me whether this is an oversight in the drafting, or a deliberate policy choice.

3.63. The conduct element of the offence is the obtaining, accepting or retaining (section 17(1), carrying a maximum of 14 years) or agreeing to accept (section 17(2), with a maximum of 10 years). The mental element is knowledge or constructive knowledge ("having regard to other matters known to them ought reasonably to know") that a FIS is a source of the delivered or promise benefit.

3.64. The purpose of the offence is undoubtedly to lessen the burden on prosecutors, and to catch precursor conduct. Instead of having to show that a defendant has carried out assisting conduct (the section 3 offence), it is sufficient to prove that a defendant has taken payment in cash or in kind[201].

- The focus will be on bank statements or cash receipts, and tracing the identity of the donor, and the defendant's awareness of the donor's identity, rather than any wider espionage activity whose nature may be impossible to put into evidential format[202].

3.65. The inclusion of **information** is noteworthy. During Parliamentary debates, the government suggested that information would be a material benefit if it had the potential to result in a financial benefit, such as business information[203].

---

[200] Section 3(5).
[201] HC (Public Bill Committee) (8.9.22), Security Minister.
[202] See for example Explanatory Notes, para 171, example 1.
[203] HC (Public Bill Committee) (8.9.22), Security Minister.

3.66. But there is nothing in the statutory language to confine information to financial tips[204]. A criminal might be induced to cooperate with a foreign intelligence service by the offer of information about him on police systems that the foreign service has penetrated, or information on the home address of his love rival. Neither of these pieces of information has financial value in a conventional sense.

3.67. The inclusion of the obtaining information pulls some obviously innocent activity into the orbit of the offence:

- The CIA, the US foreign intelligence service, has a website (cia.gov) which is accessible from the UK.
- It contains an archive of reports, including transparency reporting by the Agency on privacy and civil liberties, and country-specific reports in its "World Factbook" (which are sometimes cited in immigration proceedings in the UK).
- For the interested researcher, lawyer, or curious member of the public, this information does constitute a material benefit.
- There is no exemption for generally accessible information.

3.68. Speech offences are controversial enough since they impinge upon the currency of human interactions and political and social freedoms; an offence which impinges on the mere receipt of information is a further step beyond.

3.69. To avoid unintended consequences and unwarranted infringements of the right to receive information, the word "material" may need to carry some weight. Receiving public information from the internet might count as a benefit but not a material one.

[204] Information is defined by section 34(1) to include information about tactics, techniques and procedures.

3.70. As with the section 3 offence, extra-territorial jurisdiction applies to "UK persons"[205] who accept or agree to accept material benefits when they are overseas[206]. Criminal liability also applies where the material benefit is provided, or is to be provided, "in or from" the UK[207]. So, if a non-national makes an agreement with their local foreign intelligence service to pick up a benefit when they arrive in the UK, they commit an offence.

Defences and Exclusions

3.71. The ease with which it is possible to commit the section 3 and 17 offences in both forms puts great weight on the defences. It could be said that the defences are as important in delineating the nature of the prohibited conduct as the formal definition of the offences. I consider below whether this provides sufficient certainty.

3.72. The defences are evidential defences, meaning that if sufficient evidence is raised, it is for the prosecution to disprove the defence beyond reasonable doubt[208].

3.73. The first defence is that the defendant is acting in compliance with a legal obligation under UK law which is not a private law obligation[209]. No examples are given but this might apply to a judge whose judicial oath requires him to rule in favour of a FIS on the evidence before him. It would exclude merely contractual obligations, or obligations imposed on by foreign laws. For example, it would not excuse a national of Country A whose laws require her to cooperate with Country A's intelligence service on UK-related activities.

---

[205] Broadly speaking, UK nationals, companies or residents: see sections 17(12), 3(10), 2(6).
[206] Section 17(6)(b).
[207] Section 17(6)(a).
[208] Section 3(8).
[209] Section 3(7)(a), 17(8)(a).

3.74. The second defence is a Crown defence which exonerates officials and others who are acting in accordance with their public duty[210]: for example, UK officials who deal with FIS in the course of their work.

3.75. The third defence[211] benefits a "lawyer" carrying on "a legal activity" (both defined[212]). This is significant protection for legal activity, which applies whether or not any information is legally privileged; however, if the assistance involved the lawyer in other criminal conduct such as espionage (section 1, section 2) they would still be criminally liable for that conduct.

3.76. The fourth defence merits real attention.

3.77. It applies to a person who engages in the conduct in question, "in *accordance with,* or *in relation to* UK-related activities carried out in accordance with, *an agreement or arrangement* to which" either (a) the UK or (b) any person acting for or on behalf or, or holding officer under, the Crown, was a party[213]. This rather dense language identifies two scenarios:

- *Either* the defendants' own conduct is in accordance with a UK agreement or arrangement. For example, an agent of MI5 who is tasked to meet a FIS for the purposes of a counter-intelligence operation.
- *Or* the defendant's conduct is in relation to UK-related activities by a FIS that are carried out with the agreement of the UK. For example, the

[210] Section 3(7)(b), 17(8)(b).
[211] Section 3(7)(c). There is no equivalent under section 17 because reasonable payment for legal services would be an excluded benefit under section 17(4) which I consider below.
[212] Defined by para 6(4) of Schedule 15.
[213] Section 3(7)(d), 17(8)(d). This wording is different from the exemptions to the FIRS scheme found in Schedule 15 para 1: these exemptions only apply to foreign activity arrangements or foreign influence arrangements that "are" UK arrangements or agreements; or to activities "carried out in accordance with" such arrangements or agreements.

defendant is dealing with a foreign intelligence officer whose presence and activities have been declared to the government.

3.78. There are no formalities required for an agreement or arrangement. This was emphasized during the passage of the Bill. The Minister stated,

> "We believe that any activity taking place in the UK on behalf of a foreign intelligence service that the UK has *not even informally agreed* would be inherently prejudicial to the safety or interests of the UK." [214]

3.79. This defence could be an answer to potential liability on the part of the taxi-driver who drives a FIS to a meeting. Of necessity providing transport to a FIS will assist the FIS in their UK-related activities (noting that assistance does not have to be given to UK-related *intelligence* activities). It could be argued that the UK has given general agreement to people, including any FIS operating in the UK, using taxi cabs.

- Conversely, if the taxi driver assisted a person in covert intelligence gathering, such activity by the FIS would be outside the scope of any UK arrangement or agreement[215].

3.80. However, it would be wrong in principle for the defence to be equivalent to, "Whatever the UK authorities approve of" [216]. Whilst it will be obvious that

---

[214] Hansard (HL Committee) Vol 826 col 999 (19.12.22), Lord Murray of Blidworth.
[215] Article 3.1(d) provides that the functions of a diplomatic mission include ascertaining "by all lawful means" conditions and developments in the receiving state and reporting back to the government of the sending State.
[216] It would make the offence so vague that it would offend the rule against doubtful penalisation. This is the principle that "…a person should not be penalised except under clear law. This principle forms part of the context against which legislation is enacted and, when interpreting legislation, a court should take it into account" (Bennion, Bailey and Norbury on Statutory Interpretation 8th ed, (2020) at section 26.4) as referred to by the Supreme Court in Rakusen v Jepsen [2023] UKSC 9, at para 57.

some FIS UK-related conduct is outside the scope of any agreement with the UK (for example, engaging in sabotage), this will not always be the case.

3.81. The government's answer during debates on the Bill was to point to prosecutorial discretion[217] – certainly an important feature but one that does not apply to prior investigative or executive activity such as arrest and search.

3.82. Nor is prosecutorial discretion an answer if the defendant wishes to exercise his right to disagree with the prosecution case against him.

- By way of further example, a shopkeeper sells long-range binoculars to an embassy contact.
- The prosecution case is that the shopkeeper knew or ought to have known that the embassy contact was involved in covert espionage at that time, and that selling the binoculars was likely to constitute material assistance in surveilling military bases in the UK.
- The defendant pleads not guilty. He accepts he ought to have known that his customer was a FIS from earlier interactions, but he believed he was also a genuine bird-watcher. He also accepts that selling long-range binoculars would be likely to materially assist a FIS in carrying out UK-related activities.
- It is not at all clear in this scenario what defence might apply. Whatever the government might formally or informally agree about foreign diplomats using shops in the UK for ordinary purposes, the government would not have agreed to using shops for *this malign purpose*.

3.83. Another answer would be to expand the UK arrangements defence, so it applies to a person *who honestly believes* that her conduct is in relation to UK-related activities carried out in according with an agreement or arrangement to which the UK (or UK official) is party. But this is contrived. The

[217] Vol 826 col 999.

shopkeeper providing binoculars or the taxi-driver taking a fare is not thinking about arrangements at all. To give him a defence based on whether he suspects an arrangement to exist (whether Vienna Convention on Diplomatic Relations or some bespoke arrangement) is simply artificial.

3.84. A better answer may lie in the exclusion from liability in the section 17 offence. Expressly excluded from the concept of material benefit is benefit provided as reasonable consideration for the provision of goods and services, where the provision is not otherwise an offence (for example, drugs supply)[218]. This provides a defence to the taxi-driver, shopkeeper and cleaner if charged with obtaining a material benefit under section 17.

3.85. There is no equivalent defence in section 3, but there could be circumstances where a defendant charged with providing material assistance ought to be able to argue that he was doing *no more* than providing goods or services for reasonable consideration. If his conduct could not be prosecuted under the section 17 offence, then it is hard to see why he should remain liable under section 3 if he honestly believed that nothing sinister was going on.

3.86. I will desist from recommending a specific amendment, but I invite the government to explain how section 3 is intended to apply where a person is accused of providing material assistance to a person who he accepts is a FIS, but for non-sinister reasons.

3.87. There is a final defence to consider under section 17 which applies to *retaining* a material benefit from a FIS. A reasonable excuse defence is available[219]. This will spare individuals who received gifts from foreign intelligence services prior to the coming into force of the NSA from having to return their gifts where (for example) they have declared the payment to UK authorities.

---

[218] Section 17(4).
[219] Section 17(7).

Prohibited Places Offences (Sections 4 and 5).

3.88. The prohibited place offences are updated to deal with accessing or inspecting sensitive locations by remote or electronic means, and are not limited to cases of trespass by proximity[220].

3.89. A place is a prohibited place if it satisfies any of the definitions in section 7:

- Crown land in the UK or the Sovereign Base Areas in Cyprus used for UK defence[221] and for the purposes of defence of a foreign country or territory[222].
- Vehicles in the UK or the Sovereign Base Areas that are used for these purposes.
- Vehicles anywhere in the world that are used for UK defence purposes[223]
- Any land or building in the UK or Sovereign Base Areas used for weapons development or weapons capability for UK or foreign defence. This cannot be intended to cover public land such a National Park that is merely used from time to time for military training.
- Any land or building in the UK or Sovereign Base Areas owned or controlled, or used for the functions, of the UK intelligence agencies[224].

3.90. The definition is apt to include covert as well as overt buildings and vehicles:

---

[220] Law Commission, Final Report, para 2.12.
[221] Further defined in section 7(2). The examples given in the Explanatory Notes, para 107, are barracks, bases, naval dockyards and military headquarters.
[222] Further defined in section 7(3).
[223] For example, aircraft, vessels, submarines or tanks, or trains or convoys transporting weaponry, see Explanatory Notes, para 108.
[224] The Security Service (MI5), the Secret Intelligence Service (MI6), and GCHQ.

- It is unsurprising that some sites used by the military or intelligence agencies will be hidden from the public, but of extreme interest to foreign spies and therefore meriting protection as prohibited places.
- However, this means that the status of some land or buildings will not be clear. Any private facility used for manufacturing arms for UK or Ukrainian defence purposes would qualify but the grounds for qualification would not necessarily be obvious from the outside.
- The law leaves it open to facilities to self-declare or not[225]. There is no obligation to obtain government permission before doing so, raising the prospect of over-claiming and inhibiting otherwise lawful protest.

3.91. The Secretary of State's power to add sites by regulation under section 8 may be exercised by laying a statutory instrument before Parliament, subject to annulment by either House (the negative resolution procedure)[226]. It applies to land or buildings in the UK or the Sovereign Base Areas, or to vehicles anywhere. Civil nuclear sites that were previously designated under the 1911 Act have already been newly designated under this power[227], as has the Counter Terrorism Operations Centre in West London[228]

3.92. Designation must be necessary to protect the safety or interests of the UK having regard to the purpose for which the land, building or vehicle is used, and any information, technology, equipment or material held there[229].

3.93. Since provision is made for addition by "description" of land, building or vehicles as well as reference to particular land, buildings or vehicles, it appears that the designation instrument does not need to identify the address. So, if a

[225] See Ministry of Defence, Industry Security Notice Number 2024/03, issued 15/4/2024, paras 12 to 13.
[226] Sections 8(1), 96(4).
[227] National Security (Prohibited Places) (Civil Nuclear) Regulations 2023.
[228] The National Security Act 2023 (Prohibited Places) Regulations 2024.
[229] Section 8(2), (3).

new intelligence body was created, the Secretary of State could designate any buildings owned by this body, whether those buildings were covert or publicly avowed.

3.94. A separate and analogous power exists for police to designate cordoned areas to secure military aircraft or related equipment (sections 9-10). In practice this is to deal with crashed military aircraft. Entry into a cordoned area is not itself unlawful, but failing to comply with associated police directions (considered below) is an offence[230].

Summary Offence

3.95. The summary offence (section 5) applies to unauthorised access to a prohibited place, and is only triable in the magistrates' court, carrying a maximum 6 months' imprisonment. It only applies to conduct in the UK[231].

3.96. The offence is committed by accessing, entering, inspecting, or passing over or under the prohibited place where this is done in person (for example, using bolt-cutters to enter a site), electronically (for example, hacking a CCTV network which covers the site) or by remote means (for example, flying a drone over the site)[232]. Inspection includes taking or procuring the taking of photos, videos or other recordings of the prohibited place[233]. It does not include merely being in the vicinity.

3.97. It is also committed where a person causes an unmanned vehicle or device to access, enter, inspect, or pass or over or under the place[234]. There is potential overlap between carrying out a remote inspection via a drone and

[230] Section 11(4).
[231] There is no extra-territorial jurisdiction created by this offence: contrast section 4(4).
[232] Section 5(1)(a)(i), and the examples given in the Explanatory Notes at para 93.
[233] Section 5(3).
[234] Section 5(1)(a)(ii).

causing an unmanned drone to carry out an inspection: these different limbs may reflect the difference between the individual who has the visual feed, and a person who is just an operator of the device.

3.98. The conduct must be unauthorised, and known actually or constructively ("knows, or having regard to other matters known to them ought reasonably to know") to be unauthorised[235]. As in the trade secrets offence (section 2), conduct is "unauthorised" if the individual is not entitled to determine whether they may engage in the relevant conduct, and they do not have consent from a person who is so entitled[236].

3.99. Whether conduct is "unauthorised" is not straightforward when dealing with drones or photographs:

- Although the lawful occupant of land is entitled to determine who may enter it, including the airspace above it, this does not apply indefinitely upwards[237], so there comes a height at which flying a drone above a site will not depend on the occupant's absence of consent.
- If the drone flying is unlawful according to civil aviation regulations, the concept of "unauthorised" just about fits, assuming there are circumstances in which a public authority (such as the Civil Aviation Authority, or the Secretary of State) could give consent to the conduct. This begs the question of how drone use is regulated in the UK or not.
- A member of the public who is on public land is entitled to take photographs of land and buildings[238], so taking photographs from public land or even remote surveillance from public land could not constitute a section 5 offence. This will be a relief to tourists (and intelligence

[235] Section 5(1)(b)(c).
[236] Section 5(2).
[237] Bernstein (Baron) v Skyviews & General Ltd [1978] QB 479.
[238] Although reconnaissance photos could be useful to a terrorist and fall within sections 58 or 58A Terrorism Act 2000. See Metropolitan Police, "Photography Advice" (last accessed 5.3.24).

operatives posing as tourists) and has some relevance to 'auditors' whose activity I have considered elsewhere[239].

3.100. Section 4 could also cause injustice where the facility is covert or where it is not obvious that inspection should be avoided (for example, a UK military vehicle which is driving in a National Park)[240]. A conviction under the National Security Act 2023 would be excessive where the only culpability was curiosity without respect to the occupant's rights.

Aggravated Offence

3.101. The aggravated offence in section 4 is intended to be the real deterrent to foreign spies worldwide. It carries a maximum sentence or 14 years' imprisonment and is different from the summary offence in three ways.

3.102. **Firstly**, approaching or being in the vicinity of a prohibited place[241], and inspecting photographs, videos or other recordings that have previously been taken[242]. These conduct elements are wider than under the summary offence. They would cover approaching a UK military vessel in a foreign dockyard and the purchase by foreign spies of a house with overlook on a UK military base. But approaching or being in the vicinity of a prohibited place begs the question, "how close?".

3.103. The offence does not depend upon the conduct being unauthorised, so it includes taking photos when lawfully present on public land.

---

[239] Terrorism Acts in 2021 at 4.73 et seq.
[240] Unlike the offence of trespassing on a designated site under the Serious Organised Crime and Police Act 2005, it is no defence to prove that the individual was ignorant of, and had no reason to suspect, that the place was prohibited: see section 128 of that Act.
[241] Section 4(1)(i), (ii).
[242] Section 4(2)(b).

3.104. *Inspecting* photographs will include inspecting photographs have been commissioned for sinister purposes[243] and images that have been taken innocently by unwitting co-optees. Even in the case of foreign spies this conduct element seems overbroad as respects inspecting photographs, videos or recordings that are widely available on the internet or as part of film or TV sequences.

3.105. Indeed, the width of the conduct covered by section 4 means that the activities of legitimate journalists (as well as spies posing as journalists, or journalists funded by a foreign power) are very much within scope. Journalists expose scandals and unearth truth in the public interest with respect to military and intelligence activity just as they do with politics or business. Proper journalistic behaviour enhances oversight and public consent.

3.106. **Secondly**, unlike the summary offence, the conduct can be carried out anywhere in the world[244]. A person who flies an aerial surveillance drone over a prohibited place in the UK, whilst he is outside the UK's territorial waters, is caught[245], as is any entry onto any prohibited places worldwide (for example, an overseas military vehicle).

3.107. **Thirdly**, the conduct must be for a purpose that is known actually or constructively ("knows, or having regard to other matters known to them ought reasonably to know") to be prejudicial to the safety of the UK[246].

---

[243] The example given in the Explanatory Notes, para 92, concerns images of members of staff entering a prohibited place

[244] Section 4(4).

[245] Para 94. Arguably the conduct of drone operator would take place partially in the UK (cf. R v Sheppard [2010] 1 WLR 2779 where a substantial measure of the offence took place in the UK even though the inciting material was uploaded to a server in the UK); in any event a court might well interpret the statute as permitting extra-territorial jurisdiction in such circumstances (cf. R v Laskowski [2023] EWCA Crim 494, where an encrypted offer to supply drugs into the UK was made in the Netherlands).

[246] See further Chapter 2.

3.108. The purpose need not be espionage (it would include sabotage), nor need it be motivated by hostility to the UK in favour of a foreign power. This will cover activists who seek to damage aircraft on political disarmament grounds. There are no statutory defences. The prejudicial purpose requirement therefore carries a great deal of weight in ensuring accurate prosecution and conviction.

Police Powers in relation to Prohibited Places and Crashed Aircraft

3.109. Under section 6, police are given coercive powers backed by summary criminal sanction in relation to prohibited places. These enable officers to stop entry, inspection, approach or being in the vicinity (directly or by remote means), and to require a person in an "area adjacent" to leave the area immediately. Any power is exercisable only if the constable reasonably believes that its exercise is necessary to protect the safety or interests of the United Kingdom[247].

3.110. Protest activity outside a prohibited place is at risk. The government acknowledged this but pointed to the particular sensitivity of prohibited places[248].

3.111. "Area adjacent" is undefined and could encompass a significant patch of land. During passage of the Bill, the government claimed that it would assist hostile actors to specify a precise limit to adjacency but promised guidance to police[249]. Unpublished guidance has now been prepared by the College of Policing.

3.112. Whilst I accept that formal limits to the power might encourage adaptation by foreign agents (for example, use of high-powered binoculars with

[247] Section 6(3).
[248] HM Government, Human Rights Memorandum, para 29.
[249] Letter, Lord Sharpe of Epsom (10.1.23).

impunity), that protest activity may shade into direct action attracting less human rights protection, and that officers may need to act quickly in response to events, there are insufficient safeguards built into the legislation to prevent unjustified incursions into public protest.

3.113. It would be wrong for peaceful protesters to be shooed away from prohibited places without adequate consideration being given to freedom of expression and assembly. These democratic interests are not sufficiently articulated by the College of Policing Guidance, which is in any event unpublished and so cannot be consulted, or relied upon, by the peaceful protester. Being unpublished it will not assist the authorities in showing that any interference was "in accordance with the law"[250]. I therefore **recommend** that additional safeguards are created. Ideally this would be in the form of a public Code of Practice to which constables should have regard when exercising their powers under section 6.

3.114. Equivalent powers are given to constables[251] where an area has been cordoned under section 9 to secure military aircraft or aircraft parts within it. In practice this is intended to deal with crashes. However, a direction may be given without justification by reference to UK safety or interests; the need to keep individuals at bay from crashed military aircraft is taken for granted. In principle, it could be used to require the lawful occupant to leave his land.

Sabotage (Section 12)

3.115. Sabotage, a new offence carrying a maximum of life imprisonment, extends to any form of conduct resulting in damage to an asset where:

[250] Under general human rights principles, any interference with a right must be in accordance with the law. This implies a level of foreseeability and therefore accessibility by the affected person.
[251] By section 11.

- the individual knows actually or constructively that their conduct is prejudicial to the safety or interests of the UK, and
- the foreign power condition is met[252].

3.116. The wide scope of the offence is illustrated by six matters.

3.117. Firstly, there is very little limit to the type of asset whose damage may qualify. Asset is not limited to national infrastructure or assets owned by the government. It applies to intangible assets (such as patents) and electronic systems and information[253], and to assets anywhere in the world[254].

3.118. Secondly, it applies to conduct anywhere in the world[255].

3.119. Thirdly, the offence applies to omissions resulting in damage[256] (for example, failing to carry out safety checks on a nuclear reactor, which results in a suspected radiation leak[257]) as well as positive acts. This appears to explain why the conduct element is expressed as conduct that "results in damage to any asset"[258].

3.120. Fourthly, damage can be temporary and extends to alteration, contamination, interference, loss or reduction in access, availability, function, utility or reliability[259] (such as introducing malware into a water treatment facility[260]). It could include tampering with submarine cables carrying UK internet traffic or a foreign gas pipeline supplying UK homes and

[252] Section 12(1)(c), (d). For both these conditions, see Chapter 2.
[253] Section 12(3).
[254] Section 12(2)(b).
[255] Section 12(2)(a).
[256] Section 34(1).
[257] Example 3, Explanatory Notes para 128.
[258] Section 12(1)(a). Contrast section 1 Criminal Damage Act 1981.
[259] Section 12(3).
[260] Explanatory Notes, para 128, Example 1.

businesses[261]. It could also include political activism or damaging one's own property[262].

3.121. Fifthly, the offence may be committed by foreign citizens.

3.122. The individual must know that their conduct will result in damage or be reckless as to whether damage will result[263]. There is no defence of "lawful excuse", belief in owner's consent or reasonable defence of property rights[264].

3.123. It follows that the envelope of conduct (assets of any type, anywhere in the world, temporary impairment and reckless conduct sufficient, no defence of "lawful excuse") is very wide indeed. The additional elements of the offence are:

- Actual or constructive knowledge of purpose prejudicial to the UK;
- Satisfaction of the foreign power condition.

3.124. Since the conduct may take place abroad, the foreign power condition may present a barrier of midget proportions only.

- For example, a carpenter is employed by a regional government in France to change the plugs in the local town hall – he will damage the old plugs (there is no defence of consent), and the foreign power condition will be met.

3.125. This places the emphasis squarely on the requirement that the conduct must be done for a purpose prejudicial to the UK. Absent the need for the prosecution to show that the defendant *actually or constructively knew* of such

[261] Example 2.
[262] Human Rights Memorandum at para 37.
[263] Section 12(1)(b).
[264] As exists under section 5(2) Criminal Damage Act 1981.

a purpose, the offence would be obviously overbroad. But even with this requirement, there are scenarios that test the meaning of the word "sabotage":

- For example, an engineer working on artificial intelligence for a foreign government is instructed to destroy a prototype to avoid it falling into the hands of the UK and its allies. The defendant would know that the purpose (of keeping this powerful technology from the UK) was prejudicial to the UK – but it is hard to describe his conduct as sabotage.

3.126. Whilst the government's reluctance to create a reasonableness or lawful excuse defence is understandable[265], the offence does appear to catch some blameless conduct overseas. I intend to keep this point under review.

Foreign Interference (section 13)

3.127. The Canadian Security Intelligence Service has broadly summarised foreign interference as "attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign country" and "to covertly influence decisions, events or outcomes to better suit their strategic interests"[266].

3.128. This summary is useful because it is compendious like the foreign interference offence itself. Foreign interference under the NSA has a complicated construction and can be committed in multiple ways. There was no attempt to crystallise the essence of interference, which is prohibited under international law[267] but in practice defined in the eye of the beholder[268].

---

[265] Because of the fear of overcomplicating the offence, and the risk that hostile actors would exploit defences.
[266] 'Foreign Interference: Threats to Canada's Democratic Process', July 2021.
[267] Article 41(1) of the Vienna Convention on Diplomatic Relations (1961) places a duty on persons with immunities and privileges "not to interfere in the internal affairs of [the Receiving] State".
[268] Walker-Munro, B., '"To live convincingly": legal challenges at the intersection of diplomacy and foreign interference', Edin.L.R. 2024, 28(2), 147-173.

3.129. Foreign interference is a good example of how the NSA contains overlapping offence provisions. Conduct capable of amounting to foreign interference may also be prosecutable as another offence:

- If done at the behest of a FIS, under section 3.
- If it involves damage to property, and is prejudicial to UK safety and interests, as sabotage under section 12.
- If it involves preparing for serious violence against a person, as acts preparatory under section 18.
- If it involves unauthorised access to a computer, as an offence under the Computer Misuse Act 1990 aggravated under sections 19-22[269].

3.130. Foreign interference also stands alongside the Foreign Interference Registration Scheme (FIRS) established by Part 4 of the Act. The Scheme is outside the scope of my statutory review but is a potential alternative route to investigation and prosecution for tasked agents (individuals in a "foreign activity arrangement" with a foreign power) who might otherwise commit the section 13 offence.

3.131. The Scheme includes the enhanced tier (sections 65-8) which applies to foreign powers or individuals of particular concern as designated by the Secretary of State; and a less demanding scheme concerning political influence (sections 69-72).

- However, the FIRS regime is about registration not prohibition. Prosecution for foreign interference is a bigger stick than a technical non-registration offence[270].

[269] See Chapter 2 for the Foreign Power Condition as an aggravating factor for non-NSA offences.
[270] HC (Public Bill Committee), 12.7.22, Security Minister.

- As Paul Scott has pointed out, the FIRS scheme is not bulletproof[271].

3.132. In summary, foreign interference is a three-legged stool requiring proof of (i) "prohibited conduct", (ii) the potential for an "interference effect", and (iii) the foreign power condition. It carries a maximum of 14 years' imprisonment.

3.133. There is no additional need to prove prejudice or intended prejudice to the safety and interests of the UK. This means the offence is capable of scooping up conduct such as a single instance of attempting to intimidate a UK voter.

Interference Effect

3.134. As the Explanatory Notes illustrate, interference effects may appear in a wide range of scenarios[272]:

- An agent of a foreign power threatens a politically active member of a diaspora community to get them to return to their country of origin and renounce their political views[273]. This type of conduct is sometimes referred to as Transnational Repression[274].
- An employee of a company owned by a foreign power is instructed to obtain sensitive information on MPs which he knows could be used to affect they vote in Parliament[275].
- Employees of a troll farm are used by a foreign power to sow discord by manipulating public opinion against infant vaccines[276].

---

[271] 'State threats', security, and democracy: the National Security Act 2023', Legal Studies (2023), 1–17: "a foreign unincorporated organisation which is aligned with a foreign power and staffed by its sympathisers but not directed by it can fund political influence activities in the UK without these being registered".
[272] Para 150.
[273] Example 1.
[274] See further my speech, 'Transnational Repression: What Planet Are We On?' (The Hague, 29.5.24).
[275] This is what I understand Example 2 to entail.
[276] Explanatory Notes, para 150, Example 3.

- A foreign national living in the UK, funded by a foreign power, misleads and threatens members of her diaspora community in relation to candidates in a UK election[277].
- An individual who intimidates a juror who is trying the case of a foreign intelligence agent[278].

3.135. The statutory definition of "interference effect" has six alternative facets[279].

3.136. Firstly, interfering with the exercise by a particular person of a right under the European Convention on Human Rights[280] in the UK.

- The government referred during debates to undermining free speech and lawful protest in the UK[281].
- It will be noted that the interference is with "the exercise" not with the Convention right itself. This may be a technical point recognising that it is public authorities under the Human Rights Act 1998 rather than private individuals who interfere with rights.
- Since the exercise must be "interfered with" and not merely "affected" it is debatable whether enhancement of rights could be a basis for criminal liability under this provision[282].

3.137. Secondly, *affecting* the exercise by any person of their public functions.

---

[277] Example 4
[278] Example 5.
[279] Section 14(1)(a)-(f).
[280] Specifically, the rights scheduled in the Human Rights Act 1998.
[281] HC (Public Bill Committee), 12.7.22, Security Minister.
[282] Take for example an agent of a foreign power who provides a UK national, at his request, with a website to express her views and thus enhances the exercise of her right to freedom of expression. The ordinary meaning of interfere (in relation to a person) is entering into something without right or invitation: Shorter Oxford English Dictionary.

- The use of the word “affecting” rather than “interfering” suggests that it includes *improving* the exercise of those functions – for example, paying for a researcher for a Member of Parliament.

3.138. Thirdly, interfering with whether, or how, any person makes use of services provided in the exercise of public functions[283].

- Robert Ward gives the example of dissuading a person from cooperating with the police[284].

3.139. Fourthly, interfering with whether, or how, any person participates in UK elections or relevant political processes or makes political decisions as an elected official[285].

- Political processes are defined so they do not include proceedings in Parliament[286] (although All Party Parliamentary Committees and the like are expressly caught[287]). This is something of a cosmetic fix because the government thought that interfering with how MPs conduct themselves in debates would in any event affect the exercise of their public functions[288].
- If the prosecution alleges paid-for statements by MPs in either House, arguments about the effect of Article 9 of the Bill of Rights (which prohibits impeaching or questioning proceedings in Parliament) can be expected.

---

[283] Meaning functions of a public nature exercisable in the UK or by Crown servant anywhere in the world: Section 14(5).
[284] In ‘National Security Law, Procedure and Practice (Oxford, 2nd ed), at para 19.65. This category also applies to the example of an anti-vaccine blog given by Lord Anderson KC, former Independent Reviewer of Terrorism Legislation, and considered by the High Court in R (Miranda) v Secretary of State for the Home Department [2016] EWCA Civ 6. Whilst it would not of itself be terrorism to demonstrate against vaccination it could amount to an interference effect.
[285] Defined in section 14(4).
[286] Defined in Section 14(3).
[287] Section 14(3)(d).
[288] Hansard HL 1.3.23 vol 828 col 293, Lord Sharpe of Epsom.

3.140. Fifthly, interfering with whether, or how, any person participates in legal processes in the UK.

- This includes suborning jurors but appears wide enough to include providing funding to enable litigation, for example against the government.

3.141. Sixthly, prejudicing the safety or interests of the UK.

- This is a catchall provision. Robert Ward gives the example of a researcher at a UK armaments company who downloads sensitive designs intending to give them to a foreign power for military advantage over the UK[289].
- In 2024, the Director of GCHQ spoke of China, "...looking to shape global technology standards in its own favour, seeking to assert its dominance within the next 10 to 15 years"[290]. It is open to doubt whether a jury would be persuaded that this amounted to an interference effect if this led to better cheaper consumer electronics, and much will depend on how prejudice to UK interests can be articulated and proven in legal proceedings.

3.142. None of the categories above appear wide enough to encompass general degradation of trust as an interference effect. The Doppelganger network, sanctioned in 2024 for spreading false rumours to undermine Ukraine[291] was also reported to have spread disinformation about the Royal Family[292]. Undermining institutions, general acceptance of the current

[289] 'National Security Law, Procedure and Practice', supra, at para 19.69. He points out that this conduct would overlap with at least the offences in section 1 (espionage) and section 3 (assisting a Foreign Intelligence Service).
[290] Director GCHQ, CYBERUK speech (14.5.24).
[291] HM Government, Press release, 'UK sanctions Putin's interference actors' (28.10.24).
[292] 'Sanctions for Russian disinformation linked to Kate rumours' (BBC, 28.10.24).

democratic settlement, or simply leeching away trust in information, appears to be a project backed by certain foreign powers[293]. Research on AI-enabled disinformation as election interference has pointed towards second order degradation effects[294].

3.143. It is conceivable that causing social degradation could form part of a "course of conduct" (see further, below) with a view to achieving a later interference effect. For example:

- Aiming at voter alienation, so interfering with their participation in democratic processes.
- Affecting the ability of politicians to carry through difficult policy objectives and therefore affecting how they carry out their public functions.
- Dissuading individuals from reading and speaking about damaging behaviour by foreign states (for example, by Russia in Ukraine or China in Xinjiang Uygur Autonomous Region), so affecting the exercise of individual rights to receive and impart information.
- However, much would depend on whether there was convincing proof of an overall masterplan. Simply causing people to distrust the authorities is not an interference effect.

Prohibited Conduct

3.144. Much conduct giving rise to an "interference effect" would count as morally neutral on its own terms: for example, lobbying Ministers and thereby

[293] See OFCOM, 'Protecting People from Illegal Harms Online, Vol 2: The Causes and Impacts of Online Harm' at Chapter 6P, although the focus of this document is harms to individuals rather than harm to national security.
[294] Stockwell, S., Hughes, M., Swatton, P., Bishop, K., 'AI-Enabled Influence Operations: The Threat to the UK General Election", Alan Turing Institute (May 2024).

"affecting the exercise by any person of their public functions"[295]. What makes the real difference is the criterion, "prohibited conduct".

3.145. "Prohibited conduct" is defined in section 15 and comprises any one of the following which may be committed anywhere in the world[296]:

- Conduct amounting to an offence in the UK (of whatever gravity) or conduct elsewhere which would constitute an offence if it took place in the UK[297]. When outside the UK there is no double criminality requirement, so the conduct may be lawful in the overseas country.
- Conduct involving "coercion of any kind" [298], including violence or threats against person or property, damage or threats to damage reputation, causing or threating to cause financial loss, and "causing spiritual injury" or "placing undue spiritual pressure" on a person[299].
- "Damaging or threatening to damage a person's reputation" is designed to deal with blackmail-like behaviour, but it must reach the level of "coercion"; an important consideration since damaging and threatening reputations is the standard fare of political and online debate.
- The spiritual provisions derive from election law[300]. They could relate to excommunication or religious or spiritual curses, including coercing A by threatening to curse A's niece[301] but require careful handling to ensure that the ordinary exercise of spiritual authority is not caught[302]. It would be an egregious interference with the rights of expression, association and religion to prosecute a Rabbi or Imam under national

[295] Section 14(1)(b).
[296] Section 13(5), (6).
[297] Section 15(1).
[298] Some online interference might involve exposing truths (e.g. "doxing" a person's home address, in order to coerce them).
[299] Section 15(2).
[300] See Representation of the People Act 1983, section 114A.
[301] Section 15(2) provides that a threat to one person can be used to achieve an interference effect involving another person. For further examples of spiritual injury or pressure see Explanatory Notes, para 269.
[302] See Explanatory Notes, para 270.

security laws merely for encouraging his congregation to vote for politicians supporting Israel or Gaza.

3.146. More important than it may first appear, "prohibited conduct" also includes making a deliberate misrepresentation[303], whether express or implied, which is material to the interference effect[304].

3.147. This is crafted to catch bots, sock-puppets and other social media trickery that is pressed into service. Because "misrepresentation" includes lies about identity or purpose[305], it is particularly pertinent to the work of foreign-backed troll farms (who in future could exploit the potentials of Artificial Intelligence and Large Language Models[306]). Misrepresentation covers:

- Lies which are introduced onto social media hoping they will be amplified by innocent individuals.
- Deepfakes.
- True or false information which appears to reflect concerns of ordinary citizens, which is really a front for a foreign power – also known as "astro-turfing" and an example of what the tech companies call "coordinated inauthentic behaviour".
- True Information about historic events presented as if they have just happened.

3.148. The problem is that political debate often involves putting forward truth with a maximum of impact and "spin" which may involve actual or implied

[303] The requirement that the person knows or intends to be false or misleading was added during the passage of the Bill to avoid catching inadvertent use e.g. of false statistics: Hansard (HL) Vol 826 Col 1156 (21.12.22), Lord Sharpe of Epsom.
[304] Section 15(3) – (5). The requirement that the misrepresentation is "material to the interference effect" appears to exclude collateral untruths, although where a communication is seeking to produce a particular effect, it is quite difficult to identify any part of that communication that is truly collateral to that intended effect.
[305] Section 15(6).
[306] OpenAI, 'Disrupting malicious uses of AI by state-affiliated threat actors' (14.2.24). Its impact to date should not be overstated: OpenAI, 'AI and Covert Influence Operations: Latest Trends' (May 2024). For a more pessimistic view on the extremism front see Baele, S., Naserian, E., Katz, G., 'Is AI Generated Extremism Credible? Experimental Evidence from an Expert Survey', (2024) Terrorism and Political Violence.

untruths ("I do not recognise that assertion about my conduct" suggesting that something is untrue when it is true). Distinguishing between legitimate political dissent worthy of the highest protection and illegitimate propaganda is not always easy, and the same is true of political debate[307].

3.149. This is certainly an area where, along with former soldiers or detectives being paid by foreign powers to conduct surveillance on targets, digital marketers who are prepared to run deceptive influence campaigns, aware of or prepared to turn a blind eye to State involvement, could find themselves caught up in the crime of foreign interference.

Course of Conduct

3.150. This extended basis for liability is important.

3.151. Firstly, any "course of conduct" may involve others[308]. For example, A may threaten an MP's spouse to give up compromising information, with the intention that B will approach the MP later to influence his or her voting in Parliament. A still commits an offence even though someone else is responsible for the interference effect as part of the course of conduct.

3.152. Secondly, there is no time limit on the course of conduct and so, in principle, it can capture long-term influence operations, such as the Australian case of Di Sanh Duong[309]:

- Di Sanh Duong was a local politician and member of the Australian Liberal Party. He was convicted in 2023 of a foreign interference offence by

[307] Cf. Johnson J. in Phillips v Secretary of State for Foreign, Commonwealth and Development Affairs [2024] EWHC 32 (Admin) at para 50, citing Emerson, Freedom of expression in wartime, University of Pennsylvania Law Review 116 (1968) 975 ("dissent [can be] difficult to distinguish from actual aid to the enemy").
[308] Section 13(3), (4).
[309]

attempting to cultivate a Federal Minister on behalf of the Chinese Communist Party through making a generous and apparently disinterested donation to the Royal Melbourne Hospital in the Minister's constituency[310].

- Although there had been no attempt to influence the Minister's public functions in favour of China, the Minister had been talent spotted by Duong as a future Australian Prime Minister. Duong's purpose in league with China's United Front Work Department was to cultivate him for the longer term when presumably he would (if the plan worked) exercise his public functions in a way that assisted Chinese policy.

3.153. It is possible to envisage other slow burn influence operations which merely roll the pitch but where it might be difficult to identify an intended interference effect, let alone prove one to the criminal standard.

- If Country A took a truly long-term view and started identifying and promoting candidates for local government on the footing that they might one day "exercise public functions", "participate in relevant political processes" or "make political decisions" in a way that favoured Country A, this might suffice.
- Other forms of "elite capture" are probably out of reach. Merely cultivating a politician or senior administrator with a view to securing a yet-to-be identified advantage to Country A at some stage in the future would not amount to this offence[311].

3.154. The authorities' belief that the UK is a target for Chinese long-term influence operations has been disclosed in recent legal proceedings

[310] He was in fact convicted of *preparing* to commit a foreign interference offence under section 92.4(1) Criminal Code (Cth). HHJ Maidment's sentencing remarks of 29.2.24 are publicly available and worth considering: https://www.countycourt.vic.gov.au/files/documents/2024-02/sentencing-remarks-cdpp-v-duong.pdf.

[311] There is no offence of acts preparatory to foreign interference, butif done on behalf of a Foreign Intelligence Service, the section 3 offence would apply.

concerning the lawyer Christine Lee[312] and the businessman Yang Tengbo/H6[313].

Mental Element

3.155. The first way of committing the offence is intentionally. Here the individual intends his prohibited conduct to have an interference effect, or the "course of conduct" of which his prohibited conduct forms part to have an interference effect[314].

3.156. The second way of committing the offence is recklessly. Here the individual is reckless about whether his prohibited conduct, or the course of conduct of which it forms part, will have such an effect[315].

3.157. The third way applies where the individual engages in a course of conduct with others and knows or believes that someone else (not the defendant) will engage in prohibited conduct. The defendant must both intend the course of conduct to have an interference effect and intend or believe that someone else will engage in prohibited conduct as part of that course of conduct (recklessness not being sufficient in either case)[316].

- This catches the electrician in a troll farm run by a foreign power, if he knows or believes that it will be used to generate disinformation and intends to help create an interference effect.

[312] Lee and Wilkes v The Security Service [2024] UKIPTrib 7.
[313] Yang Tengbo v Secretary of State for the Home Department, Appeal No: SC/205/2023 (12.12.24).
[314] Section 13(1)(a).
[315] Section 13(2).
[316] Section 13(3).

Foreign Power Condition

3.158. In all cases, the foreign power condition must be met in relation to the defendant's conduct[317]. Purely domestic corruption, disinformation and election chicanery, with no foreign connection, are not caught but – especially due to the "non-contact" foreign power condition[318] – a great deal of ordinary human activity is put in scope:

- Lobbying, electioneering, journalism, marketing campaigns, humanitarian aid, social media activity are in the foreign interference zone if done with the intention of benefiting a foreign power (e.g. arms to Ukraine/ Israel; foreign aid to Pakistan; rapprochement with Russia; more access to domestic markets for Chinese cotton) so long as there is some misrepresentation (and therefore "prohibited conduct") involved.
- The conduct of foreign-funded NGOs or journalists who use deception ("prohibited conduct") to expose corrupt individuals (inevitably affecting their exercise of Convention rights) or officials (thereby affecting the exercise of their functions), could fulfil all three elements of the offence.
- The government's argument that free speech protections do not apply to journalistic activity where the FPC is met or are always outweighed by the interests of national security[319], and that (financially squeezed) journalists can always seek legal advice on the boundaries between legitimate public interest journalism and state threat activity, is not convincing.

3.159. Police and prosecutors must scrupulously avoid an arithmetical approach that merely puts together "interference effect" and "prohibited

[317] Section 13(1)(b), (2)(b) and (3)(b).
[318] See Chapter 2.
[319] HM Government, Human Rights Memorandum, paras 8, 39-40.

conduct" and "foreign power condition" and comes up with a criminal case. Just because the "three-legged stool" can be made to stand, does not mean that it should be sat on.

3.160. Although I am reasonably confident that prosecutorial discretion, recognising the good sense of juries, will ensure that borderline cases of foreign interference will not come before the criminal courts, that is not a complete answer because of the possibility of intrusive investigation and arrest; and the risk that the editors and trustees of newspapers and think tanks, to take two examples, will be stalked by fear of national security offending, and trim their conduct accordingly.

The Online Safety Act Dimension

3.161. The foreign interference offence is intended to promote online hygiene, having been added as a "priority offence" to the Online Safety Act[320]. This is directed at countering attempts by foreign state actors to manipulate the UK's information environment and undermine its democratic, political, and legal processes (including elections)[321].

3.162. In summary, foreign interference content is "illegal content"[322] and user-to-user and search services have safety duties to identify and prevent users from encountering it[323]. None of this applies to disinformation which is not connected for foreign powers[324].

---

[320] Schedule 7, para 37.
[321] Hansard (HC) Written Ministerial Statement (Chris Philp MP, Minister for Tech and the Digital Economy) (6.7.22).
[322] Section 59.
[323] For example, for user-to-user services, the safety duties under section 10.
[324] For the government's non-legislative response to disinformation generally, see for example Government Communication Service, 'Resist 2: Counter-disinformation toolkit' (2021). A useful summary of practical measures is found in Siren Associates, 'Tacking Disinformation: the EU Digital Services Act Explained' (11.11.23).

3.163. But detecting foreign interference content[325] is a complex art. The largest tech platforms have occasionally identified what they call "coordinated inauthentic behaviour" and have been prepared to attribute it to Russia and China[326]. This type of pattern analysis and evaluation[327] (with risks of false attribution) is likely beyond the capabilities of most online providers.

3.164. In practice the presence or absence of the foreign power connection may be ignored, and the focus placed on internal terms and conditions disallowing coordinated inauthentic behaviour whether foreign or domestic. Much will depend upon the approach taken by US-based tech companies to First Amendment rights to free speech and the views of the US Administration.

3.165. Without intending to criticize OFCOM, its Illegal Contents Judgment Guidance on foreign interference[328] is little more than a bare repetition of the complex statutory provisions that I have sought to analyse above. It is fanciful to believe that tech platforms, often staffed by a skeleton crew, will be poring over this summary of UK illegality. OFCOM's understanding of the risks of online foreign interference – set out in its 2023 Consultation materials[329] – is nonetheless commendable.

3.166. I remain unsure how effectively OFCOM will be able to monitor platforms' compliance with its foreign interference safety duties; and dismayed that large platforms have made it harder for the wider public, including journalists,

---

[325] Meaning content where its publication "amounts to" an offence of foreign inteference, see section 59(3) Online Safety Act 2023.
[326] Meta, 'Removing Coordinated Inauthentic Behavior From China and Russia' (27.9.22); see also Schliebs, M., Bailey, H., Bright, J., Howard, P., 'China's Inauthentic UK Twitter Diplomacy' (Oxford Internet Institute, 11.5.21).
[327] E.g. do accounts suspected of posting such content share infrastructure, have metadata in common, use a common analytics platform, amplify common narratives or websites, are they amplified in turn by state-linked entities, do they receive direction or support or oversight from state-linked entities and broader state influence apparatus.
[328] December 2024, A15.
[329] OFCOM, 'Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm' (9.11.23), at chapter 6P.

politicians, charities and pressure groups, to hold them to account by accessing data at scale[330].

Foreign interference in elections (Section 16)

3.167. The Representation of the People Act 1983 and the Political Parties, Elections and Referendums Act 2000 contain election offences of differing severity such as tampering with nomination papers or postal votes or making political donations under cover of a false identify. The effect of section 16 is to raise the various maximum penalties for these offences where the foreign power condition is met[331], resulting in higher maximum sentences from 2-7 years' imprisonment[332].

- This is different from treating the FPC as a statutory aggravating factor (under sections 19-22, above) which leaves the maximum penalty unchanged[333].
- There is an overlap of subject matter with the section 13 foreign interference offence, which carries a much higher 14 year maximum, but for section 16 it is not necessary to prove any intention or recklessness to cause an interference effect.
- Section 13 also applies outside the electoral cycle and deals with misrepresentations in elections which, perhaps surprisingly, is not generally an offence under ordinary election law[334].

[330] I refer to the withdrawal by Twitter/X of free access to its Application Programming Interface in February 2023, and by Meta's of its public insights tool, CrowdTangle in August 2024.
[331] Section 16(1)(b).
[332] Schedule 1, column 2.
[333] And therefore electoral offences under section 16 are excluded from the scope of aggravating provisions in sections 19-22.
[334] The main exception being false statements about the personal character or conduct of a candidate under section 106 Representation of the People Act 1983.

- As Paul Scott has noted, further Parliamentary efforts to use the 2023 Act to bear down on the influence of foreign money on political parties and think tanks were defeated during the passage of the legislation[335].

Preparatory Conduct

3.168. The concept of preparatory conduct, meaning precursor conduct that does not even quality as an attempt at criminal law[336], was found in predecessor legislation[337] and is also familiar in the most serious terrorism offence (attack-planning, section 5 Terrorism Act 2006).

3.169. The preparatory conduct, which can take place anywhere in the world, must be carried out with intent that one or more acts are committed[338] amounting to any of the following[339]:

- Section 1 espionage.
- Section 2 trades secrets.
- Entering etc a prohibited place contrary to section 4.
- Sabotage under section 12.
- Acts involving serious violence against or endangerment to the life of a person in the UK (but not abroad) or creating a serious public safety risk in the UK, where the foreign power condition is met.

[335] Scott, P., supra.
[336] Under the Criminal Attempts Act 1981.
[337] Section 7, Official Secrets Act 1920.
[338] Whether by the defendant, or someone else: Section 18(1).
[339] Section 18(3)-(4).

3.170. The contemplated acts need not be specific acts[340], indicating an intention to penalise individuals who are, for example, preparing for example without having yet identified a target.

3.171. Like attack planning under the Terrorism Act 2006 section 18 carries a maximum of life imprisonment[341] even though this exceeds the maximum sentence for the completed offence that may be prepared for. For example, the maximum penalty for trades secrets (section 2) is 14 years but preparing to carry out the offence carries a maximum of life. This point will no doubt be reflected in sentencing practice.

3.172. Preparatory conduct intending to commit the Foreign Intelligence Services offences (sections 3 and 17) or for the foreign interference offence (sections 13) is not included section 18. This would be unnecessary because the substantive offences already capture a wide range of preparatory conduct.

- Much preparatory conduct to do with foreign intelligence services will be within section 3.
- The "course of conduct" component of foreign interference is capable of dealing with preparatory conduct.
- Finally, what lawyers term inchoate liability (attempt, conspiracy, encouraging or assisting[342]) will apply to these offences.

3.173. It will be important to keep under review in what circumstances this offence is prosecuted. Only rarely should malign intent transform innocent conduct into severe criminal liability. Precursor liability squeezes out the

[340] Section 18(2).
[341] Section 18(6).
[342] Sections 44-46 Serious Crime Act 2007. Section 18 itself is now one of the listed offences under Schedule 3 to the 2007 Act, which means that the 2007 Act only applies where the assistance or encouragement is done with intent that preparatory conduct is carried out. Paul Scott, supra, correctly points out that inchoate liability can significantly expand the scope of the offences under the National Security Act 2023.

opportunity for people to have a change of heart and can fail to distinguish between those whose planning is lukewarm and those whose course is set.

4. ARREST AND INVESTIGATION

4.1. Though closely derived from the powers in the Terrorism Act 2000, their transposition into the NSA 2023 is complicated by the absence of a core definition, equivalent to 'terrorism' in the new legislation.

4.2. So whereas suspected terrorism and its cognates ('terrorist', 'terrorism investigation'[343]) underpin the investigative powers in the Terrorism Act 2000, the police's role under the NSA 2023 concerns suspected 'Foreign Power Threat Activity' ('FPTA') or, in the case of search warrants and disclosure orders, 'relevant acts' (as defined).

- In practice, this requires careful planning and use.
- There is little that is intuitive about the statutory threshold for these powers[344].

4.3. The risk of overreach in pursuing NSA 2023 offences will, I predict, be more apparent in investigative activity than in the criminal courts. Experience suggests that the CPS (and the Attorney General through the consent mechanism) will be cautious in bringing cases before a jury, especially because of the difficulty of proving that conduct is linked to foreign States; but there are fewer formal checks on decisions to arrest, or search, or obtain data. Examining the state threats eco-system is more likely to bring the ignorant and the careless into contact with investigative powers than counter-terrorism, and of these more are likely to be journalists, lawyers and politicians.

---

[343] Sections 32, 40.
[344] Contrast the role of 'terrorist' and 'terrorism' when considering exercise of powers under the Terrorism Act 2000.

4.4. On the other hand, investigative authorities will be keenly conscious that foreign States will be watching and that even investigative decisions, once they become public to any degree, will be evaluated for what they say or appear to say about UK intentions and capabilities[345].

Foreign Power Threat Activity (and Involvement)

4.5. Foreign Power Threat Activity (FPTA), and involvement in it, is the closest that the NSA comes to providing some sort of compendious definition of the mischief it aims at. In relation to investigations, and Prevention and Investigation Measures under Part 2, considered in Chapter 5, it has a function somewhat equivalent to "terrorism" or "terrorism-related activity" under terrorism legislation.

4.6. Under its rather sprawling definition[346], FPTA comprises one or more of the following:

- Acts constituting one of the principal offences under the Act, namely obtaining protected information or trade secrets[347], involvement with foreign intelligence services[348], entering prohibited places for a prejudicial purpose[349], sabotage[350], and foreign interference[351].

- Acts involving serious violence against another person, endangering the life of another person, or creating a serious risk to the health or

[345] UK police have operational independence from government but it is foreseeable that some States will overlook or disbelieve this aspect of the UK's constitutional model.
[346] Section 33.
[347] Sections 1-2.
[348] Sections 3, 17(1), but not the offence of agreeing to accept a benefit from a FIS under section 17(2) although such conduct would probably be caught under commission, preparation or instigation.
[349] Section 4 but not the summary-only version under section 5.
[350] Section 12.
[351] Section 13 but not electoral offences under section 16.

safety of the public or a safety of the public (so not mere public order offending, for example), where the foreign power condition is met[352].

- Threats to carry out such acts, where the foreign power condition is met.[353]

4.7. Involvement in FPTA spreads a wide net:

- Firstly, the "commission, preparation or instigation" of relevant acts or threats[354], either specifically or in general[355]. This formulation borrows from the language of terrorism legislation[356].

- Secondly, conduct that "facilitates (or is intended to facilitate)" the commission, preparation or instigation of relevant acts or threats[357].

- Thirdly, conduct which gives support or assistance to an individual P, where the person who engages in such conduct:

  (i) knows or believes P to be involved in the commission, preparation or instigation of relevant acts or threats and
  (ii) engages in the conduct for the purpose of giving support to the commission, preparation or instigation of relevant acts or threats[358].

---

[352] It will be noted that this list matches three out of the five types of acts falling within the definition of terrorism under section 1 Terrorism Act 2000 – serious damage to property and serious interference with or disruption to an electronic system are both omitted (presumably because they would be caught by the offence or sabotage or foreign interference).
[353] Section 33(3).
[354] Section 33(1)(a).
[355] Section 33(2).
[356] Sections 32(a) and (e), 36B(1)(b), 40, 57 of and various Schedules to the Terrorism Act 2000; section 4 TPIM Act 2011.
[357] Section 33(1)(b).
[358] Section 33(1)(c).

4.8. A more detailed comparison between involvement in FTPA and involvement in terrorism-related activity as defined by the Terrorism Prevention and Investigation Measures Act 2011 shows that.

- The first two categories of involvement in FTPA match the first two categories of involvement in terrorism-related activity under the TPIM Act 2011[359].
- However, one of the TPIM categories ("conduct which gives encouragement to the commission, preparation or instigation of such acts, or which is intended to do so"[360]) is omitted from the categories of involvement in FTPA. This begs the question whether the TPIM Act 2011 definition is over-inclusive or redundant.
- The final category of FTPA involvement is subtly different from its equivalent under the TPIM Act 2011. Under the TPIM Act 2011 it is enough to provide *any* type of support or assistance to individuals who are believed to be involved in the commission, preparation or instigation of acts of terrorism[361]. But for involvement in FPTA, as the Explanatory Notes recount[362], not all types of support or assistance are sufficient: the supportive conduct must be *for the purpose* of giving support or assistance to the commission, preparation or instigation of relevant acts[363].
- The thinking appears to have been – wisely – that merely providing support to a person known or believed to be involved in FTPA would cast the net too wide. Possibly because individuals involved in FTPA are more likely to lead normal and socially integrated lives than terrorists, including any type of assistance would catch the otherwise innocent caterer and cleaner and taxi driver.

---

[359] Section 4(1)(a) and (b).
[360] Section 4(1)(c) TPIM Act 2011.
[361] Section 4(1)(d).
[362] Para 305.
[363] Section 33(1)(c)(ii).

4.9. The fact that only certain offences are included in FPTA, and the subtle differences between involvement in FPTA versus terrorism-related activity, suggests that considerable thought went into when the special investigative measures should be available.

Arrest and Detention

4.10. Section 27 and Schedule 6 provide stronger powers compared to ordinary arrest powers under the Police and Criminal Evidence Act 1984. Allowing for pre-charge detention for up to 14 days[364], the basis for their exercise is that a constable reasonably suspects that an individual is, or has been, involved in FPTA.

- Justified use of the stronger powers will most likely arise in high-risk cases of investigative complexity, where release on bail prior to charge would present too high a risk to national security. Pre-charge detention may be warranted as police analyse digital media, conduct house searches, and interview suspects in order to prepare and send a file to the CPS. If charged, the individual may then be remanded into custody pending trial.
- Conversely, there may be more scope for choosing PACE arrest for some offending under the NSA 2023 because the disruptive impact of arrest on a foreign plot may be sufficient to mitigate the immediate risk.
- Arresting on suspicion for FTPA also avoid the police having to identify the precise basis for their suspicion which may be important where an investigation is based on sensitive intelligence.

[364] Part 7 of Schedule 6 allows the Secretary of State in cases of urgency to provide for detention for up to 28 days if Parliament is not sitting.

4.11. The detention regime following arrest corresponds exactly to the Terrorism Act 2000 – that is, detention for up to 14 days if authorised by warrants of further detention issued by a judicial authority (in England and Wales, where the only arrests have taken place to date, by an authorised District Judge). The Reviewer is specifically required to consider compliance with the law for individuals detained under such warrants[365].

4.12. A bespoke Code of Practice, Code I, governs detention under the NSA 2023 although it has no material difference from Code H (Terrorism Act arrests)[366].

4.13. Since the coming into force of the NSA 2023, Independent Custody Visitors (ICVs) have visited arrested individuals held at TACT Suites (whether under section 27 or PACE) as they do for terror arrestees. There are strong reasons for this continuing, and for incorporating the ICVs right to visit NSA detainees into a revised Code of Practice:

- There is general need to scrutinise this type of pre-charge detention. One detainee described this type of detention to me, I think accurately, as “eery”, involving actual or potential long periods of effective isolation in quiet and specially engineered facilities.
- Whilst an occupational hazard for intelligence officers and trained agents, at least some of those arrested will find the national security tag severely disorientating after the shock of capture wears off, and they begin to contemplate their consequences for them. One of those arrested under the National Security Act in May 2024 killed himself after charge[367].

[365] Section 64(1).
[366] SI 2024/1384 are associated regulations for video recording of interviews.
[367] https://www.bbc.co.uk/news/articles/c1vv5wlp3q5o.

- There are reciprocity considerations. Demonstrably humane treatment to NSA 2023 detainees here gives no excuse for mistreatment of UK persons arrested for espionage overseas.

4.14. I understand that the ICV Code of Practice is currently being updated to refer to the NSA 2023. I also **recommend** that section 51(1A) of the Police Reform Act 2002, which presently only refers to visit to terrorist detainees, and the provision of reports to the policing authority and to the Reviewer, should be amended to refer to NSA 2023 detainees.

Entry Search and Seizure

4.15. Unlike arrest, the power to secure entry to premises by warrant (or in cases of offence, by authority of a senior officer), or obtain confidential material through production orders, is limited to securing evidence of a "relevant act". This is similar to but not quite the same as FPTA.

4.16. Under section 23 and Schedule 2 of the NSA 2023, "relevant act"[368] means any NSA offence (apart from summary and non-compliance offences[369]):

- In addition, "relevant act" comprises any act or threat that involves serious violence to another person, endangers life, or creates a serious risk to public health or safety[370].

[368] Para 1(2).
[369] Section 5, 6, 11, or non-compliance with investigative orders granted under Schedules 2, 3 or 4.
[370] Para 1 which cross refers to sections 33(3)(b) and (c).

- Excluded from “relevant act” is any general offence, for example theft, that is merely aggravated by the Foreign Power Condition[371], leaving these to be dealt with under ordinary PACE powers (unless the offence itself involves serious violence, endangers life, or risks public health or safety).

4.17. I infer that since warrants[372] and production orders[373] may only be obtained for material that is “likely to be evidence” that “a relevant act has been or is likely to be committed”, it was thought necessary to tie the expected material to something more concrete than FPTA[374]. The effect is that these powers are somewhat narrower than their terrorism equivalents[375]. Whether this makes any practical difference to the operation of Schedule 2 remains to be seen. But as noted above, applications will need to be prepared and presented with care to avoid findings of illegality.

4.18. As with terrorism, senior officers can authorise warrants in cases of “great emergency” where “immediate action is necessary”[376]. These thresholds may be easier to identify in cases of terrorism where (generally) life and limb is at stake. Conversely there are plenty of “relevant acts” where it could be said that national security was at stake with every minute that passes – for example, a long-term influence operation – and where immediate action may be needed, but where it would be overblown to speak in terms of “great emergency”.

---

[371] Under sections 19-22. These are no offence-creating provisions but merely provide for existing offences to be aggravated for sentencing purposes.
[372] Paras 2, 9, 12.
[373] Paras 3, 4.
[374] The references are to applications in England, Wales and Northern Ireland within Part 1 of Schedule 2. Part 2 deals with applications in Scotland.
[375] Under Schedule 5 Terrorism Act 2000, an application may be made where there are reasonable grounds for believing that material is likely to be of substantial value to a “terrorist investigation” (as defined by section 32), without requiring it to be likely evidence. This opens the door more widely to certain disruptive applications – where there is little or no prospect of a prosecution because the investigation is entirely based on sensitive intelligence.
[376] Para 12.

4.19. Access to legally privileged material remains prohibited, but there are different tiers of application where "confidential material" (including journalistic material) may be sought[377]. In urgent cases where journalistic material has been seized, ex post facto authority must be obtained from a judge[378]. As the High Court has recently confirmed in an official secrets investigation[379], the protection due to journalistic material cannot be stripped away by impugning the circumstances in which it was obtained.

4.20. There has been no public confirmation of how frequently these powers have been used to date. In practice, investigators may choose to seek warrants under the NSA to warrants under PACE because they welcome the higher level of scrutiny that comes with being listed before a High Court or other senior judge and would rather front-load their preparation in high stakes cases. In addition the general post-arrest search provisions under the Police and Criminal Evidence Act 1984 are not available where a person has been arrested under section 27 NSA[380].

Disclosure Orders, Customer Information Orders and Account Monitoring Orders

4.21. All these powers are also found in the Terrorism Act 2000[381].

---

[377] Schedule 2 contains its own definition of "confidential material" (para 17(2)) which includes reference to "confidential journalistic material" under the Investigatory Powers Act 2016. By contrast, Schedule 5 to the Terrorism Act 2000 simply imports the definitions in PACE for its categories of specially protected material (see para 4).
[378] Para 13. An equivalent regime was added to Schedule 5 Terrorism Act (para 15A).
[379] R (on the application of LXP) v Central Criminal Court [2023] EWHC 2824 (Admin).
[380] Because sections 18 and 32(2)(b) depend upon arrest for an indictable offence, which section 27 is not.
[381] Schedules 5A, 6 and 6A.

4.22. To obtain a Disclosure Order there must be an investigation into property that is likely to be used for, or is the proceeds of, FPTA[382]. The hypothetical example in the Explanatory Notes[383] concerns police suspicions that a foreign saboteur is trying to obtain specialist computer equipment to damage government systems. A Disclosure Order would allow police to require information from specialist computer suppliers as part of their investigation.

4.23. For Customer Information Orders there must be an investigation into FPTA[384]. The given example concerns the need for account information on a suspected foreign agent who is thought to be making corrupting payments to UK academics working in sensitive defence research areas[385].

4.24. Account Monitoring Orders must also aid an investigation into FPTA[386]. The example given in the Explanatory Notes concerns a hypothetical investigation into foreign interference in elections[387]. Where an order is granted, it will allow the police to monitor when money is paid into a suspect account, allowing them to disrupt and/or secure evidence for a prosecution.

[382] Schedule 3 para 1.
[383] Para 224.
[384] Schedule 4 para 1.
[385] Para 235.
[386] Schedule 5 para 1.
[387] Para 245. This does not seem a good example, because the section 16 offence is not included within the ambit of FPTA, although foreign electoral interference will sometimes amount to the section 13 offence of general foreign interference.

5. CIVIL MEASURES

5.1. At the time of publication of this report, no State Threat Prevention and Investigation Measure (STPIM) has yet been made under Part 4 NSA 2023[388]. Modelled very closely on the Terrorism Prevention and Investigation Measures (TPIM) regime[389], with the equal misnomered inclusion of 'Investigation'[390], these have been identified by the government as "a measure of last resort"[391], where prosecution is not possible and no other measure would be effective against the threatened activity. Unlike the TPIM regime there is no sunset clause meaning there is no need to debate the regime every 5 years[392].

5.2. In a hypothetical example given by the government[393], an STPIM could be used on a UK national tasked by FIS to surveil London-based dissidents for future assassination or forced repatriation. If the assessment was based on highly sensitive intelligence, an STPIM could be used to keep him geographically distant from the dissidents even though prosecution would not be possible. Potential other use cases might be government officials who persistently offer confidential information or training to other governments or individuals operating aggregator sites for the leaking of government secrets.

5.3. Unlike criminal proceedings, STPIMs permit the government to rely on sensitive evidence adduced in closed proceedings from which the individual and their lawyers are excluded.

---

[388] Under section 55 the Secretary of State must make a quarterly report to Parliament on their use.
[389] TPIM Act 2011
[390] These are not investigative measures; at most the Secretary of State must consult the police whether prosecution is possible.
[391] HM Government, Factsheet dated 19.8.24.
[392] Section 21(1) TPIM Act 2011
[393] Factsheet, supra.

- This is a procedure that has operated since 2005 in connection with, first, Control Orders[394], and, latterly, TPIMs.
- A central feature of the closed regime is the presence of the Special Advocate, a security-cleared lawyer who is instructed to represent the interests of the individual during the sensitive parts of proceedings. The government should pay attention to the pay and working conditions of these lawyers - without them, the system will fall down.
- The government should also pay attention to the availability of legal aid if the individual lacks the means of private funding. TPIM experience suggests that the legal aid board do not always understand the significance of these proceedings to the individual, and the importance of representation[395].

5.4. The main criterion for making an STPIM is that the Secretary of State must reasonably believe, not merely suspect, that the individual is or has been involved in Foreign Power Threat Activity (FPTA). Any STPIM must be "necessary" for purposes of protecting the UK from the risk of acts or threats falling within the definition of FPTA[396].

- As discussed in Chapter 4, FPTA can involve non-violent activity such as espionage, assisting a FIS, and foreign interference.
- So unlike TPIMs, where the purpose is ultimately directed against the risk of tangible violence or damage or endangerment to health[397], STPIMs also deal with the risk of less tangible harms.
- Where there is a risk of foreign interference, such as a long-term convert influence operation, that harm might be very subtle. This places a significant burden on the authorities to justify any order as both a necessary and proportionate interference with the subject's rights and freedoms[398].

---

[394] under the Prevention of Terrorism Act 2005.
[395] See Terrorism Acts in 2023.
[396] Section 40(1)(3).
[397] By reference to the definition of terrorism in section 1 Terrorism Act 2000.
[398] In most cases, these will include Article 8 (private life), Article 10 (expression) and Article 11 (association).

- Respect for individual liberty means that individual measures should be the lightest and most carefully targeted of touches. But I foresee that where individuals are assessed to know tradecraft, and where it is feared that they will seek to communicate with FIS, the Secretary of State may be tempted to deploy the maximum number of measures.

5.5. Drug testing aside, the same measures are available as for TPIMS (principally, relocation in limited cases, travel, exclusion, financial, property and communications limitations, weapons, association bans, work or studies limits, reporting obligations, polygraph, appointments and tagging).

- The harshest measure, relocation, can only be ordered in cases where the feared FPTA involves violence or risk to persons or public[399]. In my report on Terrorism and State Threats I considered that this restriction could be unduly restrictive in non-violent espionage cases, and recommended that it should be abolished.
- For travel limitations, the Secretary of State is bound to publish factors to be taken into account before these are imposed[400], although she has not yet done so.
- It remains to be seen whether ideological and practical mentoring are both made available under appointment measures. The notion of ideologically de-programming a spy is an interesting one, although it cannot be ruled out that some individuals will get caught up in state threat activity on ideological or even religious grounds. From experience with TPIMs, practical mentors can counteract something of the enforced isolation that civil orders can engender.

5.6. STPIMs can be renewed for up to 5 years. In practice this means that one instance of involvement in FPTA can suffice for 5 years' worth of measures. I have already expressed my doubts in the TPIM context about this time period,

[399] Section 40(6).
[400] section 39(4).

because ministers and officials may find it tempting to conclude that if a risk previously existed, then a further extension, up to the maximum of 5 years, must be warranted.

5.7. The difficulty a TPIM subject may have in persuading the authorities that their terrorist risk has sufficiently dissipated will be readily apparent; so much the more so for state threat actors who have been trained in deception. Unlike TPIMs, where what is principally at issue is motivation to use or encourage violence, the risk posed by some STPIM subjects may be their knowledge and expertise.

5.8. This begs the question of how an STPIM subject, for example a British official with a deep knowledge of UK secrets who presents a risk of disseminating them, can ever show that his risk has diminished despite his continuing knowledge and expertise.

5.9. My experience of TPIMs suggests that the first STPIM will bring forth unexpected issues, which will give substance to future reports. I also expect that STPIMs will be used, like TPIMs, for offender management purposes on released offenders.

6. BORDERS

Introduction

6.1. Responding to the Skripal attack of 2018[401], and with the Miranda litigation firmly in mind[402], the United Kingdom's border security was further tightened with effect from August 2020[403]. New powers were conferred on police to stop and question individuals travelling through seaports and airports, or passing through the Northern Ireland border, to look for signs of "hostile activity". The government thought there might be a need to stop and question persons at pace, and analyse their devices, in the aftermath of an attack like Salisbury[404].

6.2. These new powers are found in Schedule 3 to the Counter-Terrorism and Border Security Act 2019 ("Schedule 3"), with its accompanying Code of Practice, and are familiar from Schedule 7 to the Terrorism Act 2000 whose overall framework is borrowed.

- Like Schedule 7 it is a no-suspicion power, requiring cooperation from those examined under criminal penalty for non-cooperation, permitting detention for up to 6 hours, the taking of biometrics, and the search and detention of property, typically mobile devices.
- Unlike Schedule 7 it has not been adapted to deal with small boat arrivals[405], but contains special additional provision to permit the

[401] Hansard (HC) Vol 637 Col 856 (14.3.18), Rt Hon Teresa May MP, Prime Minister.
[402] Mr Miranda was stopped at Heathrow carrying sensitive information stolen by Edward Snowden from the UK and US intelligence agencies. The use of Schedule 7 Terrorism Act 2000 powers was upheld (just about and with reservation) by the Court of Appeal in R (Miranda) v Secretary of State for the Home Department [2016] EWCA Civ 6.
[403] The biometric provisions were commenced later in Northern Ireland (June 2021).
[404] Hansard (HC) Vol 793 Col 1927, Baroness Williams of Trafford (14.11.18).
[405] Schedule 7 was amended to permit this by the Nationality and Borders Act 2022.

retention of articles which may be used for hostile purposes subject to the oversight of the Investigatory Powers Commissioner.

6.3. As successive Independent Reviewers of Terrorism Legislation have recorded in annual reports, the Schedule 7 counter-terrorism powers are amongst the strongest in the book[406]. The same is no less true of Schedule 3.

6.4. Whilst the powers can, of course, be used in a deliberately targeted manner (a) they do not have to be, and their acceptability must be tested on that basis; and (b) not having to prove justification in fine detail limits the scope for subsequent judicial review. The possibility of subsequent challenge remains a safeguard, but its scope depends on an analysis of broader themes such as the absence of bias, adherence to procedure, and use for permitted purposes rather than looking at the ultimate question of whether the particular stop and examination was justified by reference to the expected intelligence dividend.

6.5. Nonetheless, this type of power provides real tactical advantage in the hostile state activity context. Attaching a threshold (such as 'reasonable suspicion') to often fragmentary intelligence on hostile state activity as the price for conducting an examination would raise the bar too high. A no-suspicion power offers greater deterrence to hostile states who will be less able to predict when the power may be exercised, and less able to reverse-engineer grounds the intelligence leading to the stop[407], than if the police had to act on the basis of pre-formed suspicion or belief[408]. An early judicial view from the High Court of Northern Ireland is that this sort of border power is just as useful for countering hostile foreign state activity, as for terrorism, if not more; and that the need to

[406] Ranking perhaps with section 47A suspicion-free stop and search (when activated) and the use of cordons to search premises without a warrant.
[407] A point made by the Minister of State during the passage of the Bill: Hansard (HL) Vol 793 Col 1702 (12.11.18)
[408] Beghal v Director of Public Prosecutions [2015] UKSC 49.

harden the border against a repetition of the Salisbury attack was well made out[409].

6.6. Just as with Schedule 7 it is a police power. Schedule 3 examining officers are just as accountable for their decisions on the frontline as Schedule 7 examiners. Collaboration is a central aspect[410].

6.7. In preparing this Chapter I have drawn on previous reporting on Schedule 7 Terrorism Act 2000, on which Schedule 3 is based; discussions with officials; a visit to an airport in November 2024; and a periodic review of materials submitted by the Home Secretary to IPCO in connection with the retention of material; and IPCO's own reviews of Schedule 3 before the review function was transferred to my role.

Hostile Activity

6.8. The investigative target for ports powers under Schedule 3 is the presence of "hostile activity"[411]. Specifically, any examination must be,

> "…for the purpose of determining whether the person appears to be a person who is or has been, engaged in hostile activity…"[412].

6.9. Hostile activity has two cumulative components. Firstly, the activity must qualify as a "hostile act"[413] which means:

- An act that "*threatens national security*". National security is notoriously undefined as a matter of long-standing policy[414]. Considering that the UK's security and intelligence agencies have functions in matters of

[409] Nolan's application for leave to apply for judicial review [2024] NIKB 83, Scoffield J., paras 36-7.
[410] For example, through the Joint Borders Team described in Terrorism Acts in 2018 at 6.59-6.67.
[411] Section 22 and Schedule 3.
[412] Applies to examination and detention, paras 1(1), 4(1)(b); search, para 8;
[413] Schedule 3, para 1(6).
[414] Ward, R., Jones, R., 'National Security: Law, Procedure and Practice' (Oxford, 2021), at para 1.54.

national security[415], something will be a matter of national security where it legitimately attracts the interest of those agencies. The Code of Practice gives examples of espionage and troll farms[416].

- An act that "*threatens the economic well-being of the United Kingdom in a way relevant to the interests of national security*". Economic well-being is also undefined. Investigation of economic matters relevant to national security are also within the statutory remit of the agencies[417]. The Explanatory Notes refers to acts that damage the UK's critical infrastructure or disrupt energy supplies to the UK[418]; in Parliament an example was given of a banking sector employee who came across a network vulnerability that could be used to undermine confidence in the City of London to the great cost of the UK economy[419].

- An act that is an act of "*serious crime*". This means an offence for which a person of good character could reasonably expect a sentence of more than three years' imprisonment[420], or an offence involving the use of violence, or which results in "substantial gain", or is carried out "by a large number of persons in pursuit of a common purpose"[421].

---

[415] For MI5, under section 1(2) Security Service Act 1989.
[416] Annex C, paras 2, 13.
[417] Security Service Act 1989, s1(3) ("It shall also be the function of the [MI5] to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands"); Intelligence Services Act 1994, s1(2) ("The functions of [SIS] shall be exercisable only - …(b) in the interests of the economic well-being of the United Kingdom"), s3(2) ("The functions [of GCHQ]…shall be exercisable only – (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions or persons outside the British Islands").
[418] Para 139.
[419] Hansard (HC) Vol 793 Col 1927, Baroness Williams of Trafford (14.11.18).
[420] The statutory formulation omits the crucial question of whether this applies to a person who was convicted at trial or pled guilty at the first opportunity (attracting a third discount). Assuming the former, this category might realistically include conduct amounting to kidnap, blackmail, false imprisonment, robbery, and conspiracy to defraud.
[421] Para 1(7)(d).

6.10. As a result, “hostile activity” is an inclusive phrase, covering biochemical attacks all the way down to conduct where the feared harm is subtle and distant.

6.11. At the margins this activity may not be criminal at all, as recognised during the passage of the Bill[422], although the gap between criminal and non-criminal has been narrowed by the subsequent National Security Act 2023 with its broad penalisation of preparatory conduct, assistance to Foreign Intelligence Services, and foreign interference. Furthermore some of this behaviour will be activity which, if done to serve UK interests, would not just be permissible but necessary[423].

6.12. Secondly, the hostile act must be:

(a) Carried out for, or on behalf of, a State other than the United Kingdom[424], or

(b) Otherwise in the interests of a State other than the United Kingdom. There is no requirement that the person intends to benefit the foreign state, nor is it sufficient that such an intention is present: the question of whether these interests are being served is an objective one.

6.13. Taken together this definition of hostile activity covers each of five categories of harm identified in the government’s 2021 consultation on

[422] Hansard (HC) Vol 793 Col 1927, Baroness Williams of Trafford (14.11.18). Lord Anderson KC drew attention to conduct that was ‘perfectly lawful under the law of the land’: Hansard (HL) Vol 793 Col 1928.
[423] Omand, D., ‘Examining the Ethics of Spying: A Practitioner’s View’ in ‘National Security Intelligence Activity and the Just Intelligence Theory’ Criminal Law and Philosophy (2024) 18:805–818. Obtaining information on other states, even covertly, is engaged in by the UK and its allies as a matter of course and in some cases may be mandated or encouraged by international law: Ratner, S., points out in ‘Espionage, Secrecy, and Institutional Moral Reasoning’, Criminal Law and Philosophy (2024) 18:819–832, that states are encouraged to monitor nuclear non-proliferation, to report on war crimes, and to distinguish between military and non-military targets in time of warfare.
[424] Includes government, or organ, of a State: para 1(7)(b). State includes territory: para 1(7)(c).

legislation for state threats[425]: (i) physical threat to people, (ii) physical threat to things, (iii) espionage, (iv) interference and (v) "threats to geostrategic interests".

- This final category is said to include challenge to the rules-based international order through "covert means and intelligence techniques rather than legitimate diplomatic engagement".
- According to 2024 comments by the director of GCHQ, China has been "looking to shape global technology standards in its own favour" in order to achieve dominance in the next 10-15 years[426].
- In more homely terms, it is attempting to rewrite the rulebook, buy the league and recruit our own coaching staff.

6.14. The foreign State may be entirely ignorant of the act since it is "immaterial…whether a State for or on behalf of which, or in the interests of which, a hostile act is carried out has instigated, sanctioned, or is otherwise aware of, the carrying out of the act"[427]. Among other things, this allows examination in cases where a person is intending to sell UK secrets but has yet to contact a foreign State.

6.15. Finally, there is no requirement that the hostile act is in the interests of a foreign state in way that is relevant to *its* national security.

- For example, it is in interests of Country A to advance to the Quarter Finals of the World Cup. If Country A were to send an agent to break the leg of England's leading goal scorer, that would therefore count as involvement in hostile activity (under the serious crime limb) even

[425] Available online as part of the Home Office consultation documents updated 12.7.22.
[426] Speech, CyberUK 2024 (Birmingham, 14.5.24).
[427] Para 1(7)(a)(ii).

if it could not sensibly be said that getting a quarter final place was a matter of Country A's national security.

Engagement in Hostile Activity

6.16. Under Schedule 3 a person may be engaged in hostile activity even though unaware that their activity is hostile activity[428].

- So a person could be examined on account of their wholly inadvertent and morally blameless conduct.
- Examples could include a journalist carrying confidential information whose significance to national security he did not understand, or the victim of planted material. The examining officer could act if there was no possibility that the person was aware that its dissemination might be in the interests of a foreign state, or even that they were carrying the material.
- The Code of Practice to Schedule 3 refers to the innocent dupe, who "…may believe that they are working for a legitimate business, or charity, which is in fact being utilised specifically for the purpose of espionage"[429].

6.17. Since hostile activity does not require any knowledge or tasking by a foreign state[430], the phenomenon of double-ignorance could arise. A person may be engaged in hostile activity if they do something which, unknown to them threatens, national security and which is in the interests of another State, also entirely in the dark. For example:

---

[428] Para 1(7)(a)(i). Contrast Schedule 7, where there must be at least possibility that the examined person is a "terrorist" (see para 2(1) cross-referring to section 40(1)(b)) which connotes some degree of awareness (see R (Miranda) v Secretary of State for the Home Department and Commissioner of Police for the Metropolis [2016] EWCA Civ 6 at paras 53-56).
[429] Annex C.
[430] See REF above.

- The developer of an app, whose selling point is end-to-end encryption which would make it more difficult for UK security and intelligence agencies to monitor communications. It is a reasonable assumption that this would be in the interests of a foreign state even if though the foreign state has never contemplated this potential advantage.
- The lobbyist for a foreign firm, who seeks to persuade an electronic chip manufacturer to build its factory in France rather than the UK. This would engage the UK's economic well-being in a way relevant to national security even though France is entirely unaware of the lobbying and the lobbyist is only doing his normal day job.
- A journalist carrying information that is personally embarrassing to the Prime Minister on the eve of an important treaty negotiations affecting UK security interests.

6.18. In each of these cases the motive of the app developer/ lobbyist/ journalist may be more sinister than first appears, so permitting an officer to examine whether the individual is a witting or unwitting agent of a foreign state might be described as necessary in the right circumstances. Serious responsibility is placed on police to use the power wisely.

Examination of Persons

6.19. It would be naïve to suggest that there is a typical terrorist. Nonetheless the profile of individuals examined under Schedule 3 may prove to be broader than Schedule 7 examinees. Foreign agents may use sophisticated cover; their targets, facilitators and co-optees may well occupy high status positions. It is

foreseeable that examinees will include the businessman, journalist, lawyer and politician[431].

6.20. A comparatively early indication of the utility of Schedule 3 came in the exclusion case of the businessman Yang Tengbo (initially known as 'H6'). This Chinese national's dealings with Prince Andrew were shown to be covertly conducted on behalf of the United Front Work Department of China, and the Secretary of State was entitled to fear that the relationship could be leveraged for political interference purposes[432]. Significant evidence had been obtained from Tengbo's examination under Schedule 3 in 2021 which established his links to the UFWD and the existence of tasking ('talking points') on how the relationship with Prince Andrew should be conducted[433].

6.21. The Joint Committee on Human Rights was of the view that there was an even greater risk of arbitrary use of Schedule 3 than of Schedule 7, owing to the broader and more ambiguous definition of "hostile activity" (than of terrorism)[434]. I would develop the point further:

- For Schedule 7, the examining officer must at least have in mind the possibility that the examined person is morally blameworthy. That arises from the statutory question: whether the individual is a person "…is or has been concerned in the commission, preparation or instigation of acts of terrorism"[435].
- By contrast, under Schedule 3 a lawful examination may take place, with all the intrusion and inconvenience attached, of an individual for whom the question of moral fault does not arise at all.

---

[431] Cf. Hansard (HL) Vol 793 Col 1888 (14.11.18), Minister of State.
[432] H6 v Secretary of State for the Home Department, Special Immigration Appeals Commission, Appeal No: SC/205/2023 (12.12.24).
[433] Paras 113, 116.
[434] 'Legislative Scrutiny: Counter-Terrorism and Border Security Bill', 10 July 2018, HL Paper 167 of session 2017–19, p 33.
[435] Schedule 7 para 2(1) referring to section 40(1)(b) Terrorism Act 2000.

6.22. Having said this, I am not yet able to draw any practical conclusions from this conceptual distinction. Firstly, most examinations are likely to be directed at the issue of witting or witting participation, which incidentally puts a premium on human as well as digital interrogation. Secondly, the possibility that an examinee is *in fact* entirely innocent also arises under Schedule 7. I will therefore keep under review whether this needs to be reflected in the Code of Practice[436], but make no recommendation at this stage.

6.23. When the Bill was introduced, the government expected that the annual use of the Schedule 3 power would be "very low"[437]. I can report that Schedule 3 is indeed being used less frequently than its equivalent under the Terrorism Act 2000.

6.24. As with Schedule 3, there are criminal penalties attached to non-compliance. In March 2024, an individual was convicted of wilfully failing to comply with his examination at Manchester Airport by refusing to provide the PIN code to his two devices, contrary to Schedule 3 para 23[438].

Access to electronic data

6.25. Access to digital evidence is likely to remain, as with Schedule 7, a major benefit to investigators. With larger storage, examinations are likely to get longer, and detention, which is mandatory after 1 hour of examination, more likely. The question of how to enable lawful access to remotely stored data, accessible from devices but not present on them, remains under consideration[439].

---

[436] In the sense that a failure to act in accordance with the Code of Practice is unlawful. By para 56(2), an examining officer must act in accordance with it.
[437] Home Office, Impact assessment (9.5.18).
[438] R v Adam Karim (Westminster Magistrates' Court, 21.3.24).
[439] Cf. Terrorism Acts in 2021 at paras 4.22-4.39.

Retention and copying: non-confidential material

6.26. Schedule 3 includes and extends the purposes found in Schedule 7 for which material may be retained and copied. As well as the power to retain for examination up to 7 days, for use in evidence in criminal proceedings, and for use in connection with a deportation decision by the Secretary of State[440], two additional purposes are introduced[441].

6.27. Firstly, an article may be retained while the officer believes that it could be used in connection with the carrying out of a "hostile act"[442]. A threshold of positive belief is thus introduced, although since information is the currency of hostile acts, once the belief is formed this power is apt to include all digital devices as well as potential poisons. During the Bill, the government referred to "…hostile agents…trying to leave the UK with information detailing live UK intelligence agency operations, capabilities and employees"[443].

6.28. Secondly, it may be retained while the officer believes it is necessary to do so for the purpose of preventing death or significant injury (whether at home or abroad). This appears to contemplate a seized article being used for dangerous ends outside the ambit of hostile state activity, for example in organised crime activity unconnected to national security.

6.29. The retention regime is subject to oversight by the Investigatory Powers Commissioner that may be characterised as strong: the Commissioner has the power to issue binding determinations, and has to decide for himself whether reasonable grounds exist to believe that the article has been or could be used in connection with carrying out a hostile act, or could result in death or serious

[440] Para 11(2)(a)-(c) corresponding to identically numbered paragraphs under Schedule 7.
[441] Para 11(2)(d), (e).
[442] For the meaning of hostile act see 6.9 [CHECK REF] above.
[443] Hansard (HL) Vol 793 Col 1888 (14.11.18), Minister of State.

injury if returned to the person from whom it was taken, and may impose conditions or order destruction[444].

6.30. Subject to the Code of Practice, officers may also make and retain copies. As well as retaining for as long as necessary for the purposes of the examination, for use in evidence, and in connection with a deportation decision, there are two additional purposes which are broadly equivalent to the additional grounds for retention.

- Retention "while the examining officer believes it necessary to retain the copy – (i) in the interests of national security (ii) in the interests of the economic well-being of the United Kingdom so far as those interests are relevant to the interests of national security, or (iii) for the purpose of preventing or detecting an act of serious crime"[445].
- Retention "while the examining officer believes it necessary to retain the copy to prevent death or significant injury"[446].

6.31. There is a significant point of interaction between retention and copying. With digital capacity and encryption comes the possibility that copying a device may take longer than 7 days.

- Retention is permitted for the purposes of examining whether the person is involved in hostile activity for up to 7 days[447], but Schedule 3 is silent about retention beyond that period for the purposes of copying.
- After 7 days, each of the bases for further retention implies that the officer will have been able to form some view of its contents[448], but this

[444] Para 12(3)-(6).
[445] Para 17(3)(d).
[446] Para 17(3)(e).
[447] Para 11(2)(a).
[448] With one exception. Where a person has failed to comply with the examination, resulting in a charge under para 23, then retention of a digital device for longer than 7 days may be needed for use as evidence in criminal proceedings even though access has not been gained.

will not necessarily have been possible for large devices where copying is necessary before any examination of its contents can take place.

- As I have already observed in the context of Schedule 7, there is a need to consider the impact of large capacity phones on ports powers, and to recognise that technological changes may distort their operation in terms of detention of persons as well as retention of articles[449].
- I will however desist from making any recommendations until the recommendations in the Investigatory Powers Commissioner's own review of Schedule 3 have been considered.

Retention and copying: confidential material

6.32. Schedule 3 provides powers of extra intrusion into "confidential material" meaning confidential journalistic material[450], legally privileged material, confidential health records and human tissue[451]. These powers, accompanied by special accompanying safeguards, are not found in Schedule 7. Their presence was justified in Parliament by reference to the use by foreign intelligence officers and their agents of professional cover including journalists and lawyers[452].

6.33. Materials carried by Parliamentarians are not specifically addressed. I intend to keep this point under review, noting the difficulty in drawing boundaries. Would a category of parliamentary material be defined by reference to the person carrying it or the nature of the material? Would it apply only to the Westminster Parliament or also to devolved legislatures?

---

[449] Terrorism Acts in 2023 at REF [when published].
[450] Within the meaning of the Investigatory Powers Act 2016 (see section 264(6) and (7) of that Act): para 12(10)(a).
[451] Protected material as defined by section 11(1)(a) and (b) PACE: para 12(10)(b) and (11). Similar protection for confidential business records was originally in Schedule 3 but was removed (as it had been for Schedule 7) by the NSA 2023.
[452] Hansard (HL) Vol 793 Col 1888 (14.11.18), Minister of State.

6.34. These powers of intrusion may only be exercised with permission of the Investigatory Powers Commissioner, unless the urgency provisions are in play[453]. Retention and use of an article, or retention and use of a copy, may be authorised by the Commissioner if, in addition to being satisfied of the basic grounds[454], he is also satisfied that arrangements are place for secure retention, and that any use will be necessary and proportionate for a relevant purpose[455].

6.35. These measures reflect the conclusion of the *Miranda* litigation, that journalistic material should not be seized for national security purposes absent adequate safeguards against arbitrary exercise of the power. The Court of Appeal noted that "the most obvious safeguard" would be "some form of judicial or other independent and impartial scrutiny conducted in such a way as to protect the confidentiality of the material"[456].

Examination of Freight

6.36. The purpose of examination of goods is to determine "…whether they have been used in connection with a person's engagement in hostile activity"[457]. There are equivalent powers in Schedule 7, but the additional intrusive powers relating to confidential material also apply where goods are examined under Schedule 3[458].

---

[453] Para 14, after which the Commissioner must be informed.
[454] I.e. potential use in connection with a hostile act or risk of death or significant injury in the case of articles; and of necessity to retain for national security, interest of economic well-being relevant to national security, preventing or detecting serious crime, and preventing death or significant injury, in the case of copies.
[455] Para 12(5); para 18(5). Relevant purposes are national security, interest of economic well-being relevant to national security, preventing or detecting serious crime, and preventing death or significant injury: para 12(9). See also Code of Practice, para 91.
[456] Miranda, supra, at para 119.
[457] Para 9(1). The equivalent test under Schedule 7, para 9(1), is whether the goods have been used in the commission, preparation or instigation of terrorism.
[458] Paras 11(1)(c); 17(2)(c).

7. RECOMMENDATIONS

Chapter 1

I **recommend** that the Secretary of State identifies a date before, or a time period within which, official statistics on the use of State Threat powers should be published.

Chapter 3

I **recommend** that public guidance on peaceful protest should be drawn up for police officers exercising their powers under section 6 National Security Act 2023.

Chapter 4

I **recommend** that section 51(1A) of the Police Reform Act 2002, which presently refers to independent custody visits, and the provision of reports to the policing authority and to the Independent Reviewer in terrorism cases, should be amended to refer to arrests in National Security Act 2023 cases.

E03512978
978-1-5286-6138-6