Intelligence and Security Committee of Parliament

Iran

Chairman:
The Rt Hon. the Lord Beamish PC

HC 1116

Intelligence and Security Committee of Parliament

Iran

Chairman:
The Rt Hon. the Lord Beamish PC

Presented to Parliament pursuant to sections 2 and 3
of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on
10 July 2025

HC 1116

Any enquiries regarding this publication should be sent to us via our webform at isc.independent.gov.uk/contact

This publication is also available on our website at: isc.independent.gov.uk

ISBN 978-1-5286-5785-3

E03390063 07/25

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

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. the Lord Beamish PC (Chairman)

The Baroness Brown of Cambridge DBE FREng FRS

Peter Dowd MP

Richard Foord MP

The Rt Hon. Sir John Hayes CBE MP

Jessica Morden MP

Derek Twigg MP

Admiral The Rt Hon. Lord West of Spithead GCB DSC PC

The Rt Hon. Sir Jeremy Wright KC MP

This Report is the result of an Inquiry conducted by the previous Committee, which sat from July 2020 to May 2024:[*]

The Rt Hon. Sir Julian Lewis MP (Chairman)

Dame Angela Eagle DBE MP
(from 16 January 2024)

The Rt Hon. Maria Eagle MP
(from 9 February 2022 until 8 September 2023)

The Rt Hon. Sir John Hayes CBE MP

The Rt Hon. Stewart Hosie MP
(until 14 December 2022)

The Rt Hon. Dame Diana Johnson DBE MP
(until 14 January 2022)

The Rt Hon. Kevan Jones MP
(now The Rt Hon. the Lord Beamish PC)

The Rt Hon. Mark Pritchard MP
(until 22 January 2022)

Colonel The Rt Hon. Bob Stewart DSO MP
(from August 2020)

The Rt Hon. Owen Thompson MP
(from 7 February 2023)

The Rt Hon. Theresa Villiers MP[♦]

Admiral The Rt Hon. Lord West of Spithead GCB DSC PC

The Rt Hon. Sir Jeremy Wright KC MP
(from 9 February 2022)

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK Intelligence Community. The Committee was originally established by the Intelligence Services Act 1994 and was reformed, and its powers were reinforced, by the Justice and Security Act 2013.

[*] The current Committee was appointed in December 2024. The Committee has finished the Report which had been written by the previous Committee and had reached the final stage of the redactions process prior to the July 2024 General Election.

[♦] The Rt Hon. Theresa Villiers MP recused herself from the Intelligence and Security Committee's Inquiry into national security issues relating to Iran. Ms Villiers regularly makes public statements on Iran and was mindful of the constraints that being involved in the ISC's Iran Inquiry would place on her ability to continue to do so. Ms Villiers was therefore not involved in any stage of the Committee's Inquiry.

The Committee oversees the intelligence and security activities of the Agencies,[‡] including the policies, expenditure, administration and operations of MI5 (the Security Service), MI6 (the Secret Intelligence Service or SIS) and GCHQ (the Government Communications Headquarters). The Committee also scrutinises the work of other parts of the Intelligence Community, including the Joint Intelligence Organisation (JIO) and the National Security Secretariat (NSS) in the Cabinet Office; Defence Intelligence (DI) in the Ministry of Defence (MoD); and Homeland Security Group (HSG) in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. Members are appointed by the Houses of Parliament, having been nominated by the Prime Minister in consultation with the Leader of the Opposition. The Chair of the Committee is elected by its Members.

The Members of the Committee are subject to section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties. The Committee sets its own agenda and work programme, taking evidence from Government Ministers, the Heads of the intelligence and security Agencies, senior officials, experts and academics as required. Its Inquiries tend to concentrate on current events and issues of concern, and therefore focus on operational[§] and policy matters, while its annual reports address administration and finance.

The reports can contain highly classified material, which would damage the operational capabilities of the intelligence Agencies if it were published. There is therefore a well-established and lengthy process to prepare the Committee's reports ready for publication. The Report is checked to ensure that it is factually correct (i.e. that the facts and figures are up to date in what can be a fast-changing environment). The Intelligence Community may then, on behalf of the Prime Minister, request redaction of material in the Report if they consider that its publication would damage their work – for example by revealing their targets, methods, sources or operational capabilities. The Committee requires the Intelligence Community to demonstrate clearly how publication of the material in question would be damaging, since the Committee aims to ensure that only the minimum of text is redacted from a report. Where the Committee rejects a request for material to be redacted, if the organisation considers that the material would cause serious damage to national security if published, then the Head of that organisation must appear before the Committee to argue the case. Once these stages have been completed, the Report is sent to the Prime Minister to consider. Under the Justice and Security Act 2013, the Committee can only lay its reports before Parliament once the Prime Minister has confirmed that there is no material in them which would prejudice the discharge of the functions of the Agencies or – where the Prime Minister considers that there is such material in the Report – once the Prime Minister has consulted the Committee and it has then excluded the relevant material from the Report.

[‡] Throughout the Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees; the term 'Agencies' refers to MI5, SIS and GCHQ as a collective; and the term 'Departments' refers to the intelligence and security parts of the Ministry of Defence, Cabinet Office and the Home Office (DI, JIO, NSS and HSG) as a collective, unless specified otherwise.

[§] The Committee oversees operations subject to the criteria set out in section 2 of the Justice and Security Act 2013.

As part of this process, pursuant to section 3(4) of the Justice and Security Act 2013, following consultation between the Prime Minister and the ISC, the ISC has redacted content from this Report on the basis that the Prime Minister considers that the material will be prejudicial to the continued discharge of the functions of the Security Service, the Secret Intelligence Service, the Government Communications Headquarters or any person carrying out activities falling within the Memorandum of Understanding agreed with the Committee.

The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted: redactions are clearly indicated in the Report by ***. This Report also includes some redactions that have been made on *sub judice* grounds or as a result of ongoing police investigations. These are indicated by ★★★ in the text. This means that the published Report is the same as the classified version sent to the Prime Minister (albeit with redactions).

CONTENTS

THE SCOPE OF THE INQUIRY

1. The Intelligence and Security Committee of Parliament (ISC) is the only body that has regular access to protectively marked information that is sensitive for national security reasons, such that it is in a position to scrutinise effectively the work of the security and intelligence Agencies and of those parts of Departments whose work is directly concerned with intelligence and security matters.[1] The ISC is therefore an essential part of the UK democratic system, providing a vital check and balance to ensure that secret organisations and their activities are accountable to Parliament and the public for the action being taken in their name.

2. The Committee has previously considered the state threats posed by Russia[2] and by China[3] and began this Inquiry into the state threat posed by Iran in August 2021. A substantial volume of written evidence has been considered and numerous evidence sessions held with a range of witnesses. We are particularly grateful to those outside the Intelligence Community – in particular Professor Ali Ansari, Baroness Ashton of Upholland, Ambassador John Bolton, Sir Richard Dalton, Professor Anoush Ehteshami and Dr Sanam Vakil – for volunteering their insights and expertise on Iran, which provided an invaluable foundation for the Inquiry.

3. The Committee concluded its evidence-taking before Hamas's terrorist attack on Israel on 7 October 2023. This Report does not therefore consider the attack or any of the subsequent events. It also does not assess whether there has been a change in the Iranian threat to the UK or UK interests as a result. The Report does not examine whether the attack had a connection to Iran: however, we do note that Iran has historically provided Hamas with weapons, cyber assistance and financial support.

4. The Report focuses on the key elements of the Iranian threat to the UK and UK interests, including assassination and kidnap, the nuclear programme and espionage, and then examines how the Intelligence Community are responding to these challenges.

[1] Other bodies such as the Investigatory Powers Commissioner's Office and the National Audit Office have regular access to protectively marked information within their specific oversight functions.

[2] *Russia*, HC 632, 21 July 2020.

[3] *China*, HC 1605, 13 July 2023.

EXECUTIVE SUMMARY

Iran

The Iranian regime's fundamental objective is to ensure the survival and security of the Islamic Republic, which was founded in 1979 following the Iranian Revolution. This shapes – directly or indirectly – all of its actions.

Iran has an acute historical sense of vulnerability and believes that it can rely only on itself. As a result, beyond the survival of the regime, it has three key regional aims – to be a leading regional power, to contain perceived Western influence and hostility, and to protect Shi'a communities and sites across the Middle East. It also maintains a fierce, ideological hostility to Israel – regarding it as its arch enemy – that is part of the regime's DNA.

Iran's focus on survival means it is flexible, pragmatic and transactional – including in relation to its international partnerships: it is prepared to work with other state threat actors such as China and Russia if it sees a benefit for itself in doing so, as reflected in its recent support for Russia's war in Ukraine.

Iran's doctrine of 'strategic depth' – avoiding direct conflict with superior conventional powers and ensuring it does not enter into conflict within its own borders – has led it to develop 'asymmetric' capabilities such as offensive cyber and a network of regional militant and terrorist organisations across the Middle East which can undertake hostile activity on its behalf, providing it with a deniable means of threatening its adversaries. Iran has also sought to maintain the option of developing nuclear weapons as the ultimate security guarantee.

"They are there across the full spectrum of the kinds of threats we have to be concerned with."[4]

5. Iran poses a significant threat to the UK. Iran believes the UK to be a significant adversary – albeit one that sits behind the United States (US), Israel and Saudi Arabia – opposed to the Iranian regime's values and seeking regime change in Iran. Iran's main strategic objectives towards the UK include: reducing the UK's military presence in the region; undermining the UK's relationships with the US and Israel; weakening the UK's security relationships in the Middle East; and silencing criticism of Iran, either from the UK directly or from those residing in the UK.

6. The Iranian threat is more narrowly focused and opportunistic than the more strategic, all-encompassing and well-resourced threats from Russia and China. However, the Iran threat should not be underestimated: it is persistent and – crucially – unpredictable. While Iran is fundamentally a rational actor, it does not always appear to act in a coherent way and is prone to misunderstanding actions that others take.

[4] Oral evidence – Director General MI5, *** June 2023.

7. Iran's intelligence services are "*ferociously well-resourced*" by comparison with its size and economy, and have significant areas of asymmetric strength – notably cyber.[5] Iranian espionage poses a significant threat to the UK and its interests, albeit as a target the UK appears to remain just below the US, Israel and Saudi Arabia. However, it should be recognised that this prioritisation could change rapidly in response to geopolitical events. Moreover, the competition, tension and disagreement between the organisations contribute to a worrying volatility around their activity.

8. Iran has a high appetite for risk when conducting offensive activity, which means it poses a dynamic and erratic threat. For example, although Iran generally favours what it considers to be a proportionate, reciprocal response, it can nevertheless escalate action sharply with little warning. This was seen following the 2022 protests in Iran, when there was a significant increase in the threat of a physical attack to individuals in the UK and the Middle East whom Iran perceives to be a threat to the regime. Notably, Iran does not see attacks on UK-based targets as constituting attacks on the UK – the UK is simply seen as collateral in Iran's handling of internal matters (i.e. removing perceived enemies of the regime) on UK soil.

9. A further complicating factor is that, as part of its 'forward defence' policy, whereby it seeks to avoid entering into conflict within its own borders, Iran often operates through proxy groups – including criminal networks, militant and terrorist organisations, and private cyber actors. This provides it with a deniable means of attacking its adversaries with minimal risk of retaliation. As Iran does not always maintain direct control of these groups, their activities (whether at Iran's behest or not) risk escalating aggression, particularly in the Middle East region. Militant and terrorist groups in the Middle East which have a relationship with, and to varying degrees receive support from, Iran include Al-Qaeda, Kata'ib Hizbollah in Iraq, Lebanese Hizbollah and Hamas. This support may include training, lethal aid, funding and, in some cases, direction via its intelligence agencies, in particular the Islamic Revolutionary Guard Corps (IRGC).

10. In terms of the specific elements of the threat which Iran poses to the UK and UK interests:

- **Physical attacks**: The threat to opponents of the Iranian regime residing in the UK is "*the greatest level of threat we currently face from Iran*".[6] It is on a broadly comparable level to that posed by Russia. Iran uses assassination as an instrument of state policy – targeting dissidents is a high priority for both the Ministry of Intelligence and Security (MOIS) and the IRGC. Iran has a higher risk appetite *** when it comes to physical attacks – there have been at least 15 attempts at murder or kidnap against British nationals or UK-based individuals since the beginning of 2022.
- **Nuclear**: Iran proceeding with its nuclear weapon programme represents a critical threat to the UK's national security, and to global security more broadly – with the potential for regional nuclear proliferation and exacerbated regional instability.

[5] Oral evidence – Chief of SIS, *** June 2023.

[6] Oral evidence – Director General HSG, 21 June 2023.

It appears that Iran has not yet developed a nuclear weapon or taken a decision to produce one, but it maintains the option of developing one – largely as the 'ultimate security guarantee'. It is difficult to determine what would trigger such a decision by the Supreme Leader: it is plausible that Iran's intent is to maintain a state of 'nuclear ambiguity' at the threshold of weaponisation. However, it may choose to weaponise if it feels it is facing an existential threat. It is notable that since the US's withdrawal from the Joint Comprehensive Plan of Action (JCPOA) nuclear agreement in 2018, the Iranian nuclear threat has increased as Iran has taken non-compliant steps in developing its nuclear programme. While it appears that it is still short of the 'weaponisation' phase, Iran nevertheless has the capability to arm in a relatively short period – possibly *** to produce a testable device and *** to develop a deliverable nuclear weapon.

- **Espionage**: Until the recent sharp increase in the threat from physical attacks, espionage was viewed as the most serious threat from Iran – and, as noted above, it still poses a significant threat to the UK and its interests. It is focused on supporting Iran's primary objective of regime survival and stability, and is at times opportunistic in nature. Iran uses both cyber capabilities and human agents: however, the Iranian espionage threat is substantially narrower in scope and scale, and less sophisticated, than that of Russia and China. The Iranian espionage threat manifests acutely in the cyber domain, since cyber espionage represents an easier way for Iran to gain information which it would not necessarily be able to obtain within the UK due to the relatively difficult operating environment.
- **Offensive cyber**: Iran is a "*capable and aggressive cyber actor*".[7] It uses its extensive cyber capabilities for disruptive and destructive effect, conducting operations to attack and contain Western and regional adversaries without having to resort to conventional military action. At present, it appears that the UK is not a top priority for Iran in conducting such attacks; however, this could change rapidly in response to regional or geopolitical developments. The UK must therefore both 'raise the resilience bar' to improve its cyber security generally, and 'raise the cost' to Iran of it launching a cyber-attack on the UK (for example by publicly attributing such attacks), so as to deter it from doing so.
- **Interference**: While Iran does seek to conduct political interference activity (or 'cognitive warfare') – and the UK is a high priority target due to its role in multilateral negotiations relating to Iran and the presence in the UK of Iranian news outlets critical of the regime – it has had a negligible effect on UK public opinion and decision-makers, including in relation to UK elections. Of greater concern are Iran's attempts to intimidate Iranian dissidents and employees of media organisations – such as Iran International – in the UK and beyond. Some reports suggest these efforts to intimidate the regime's perceived opponents have had a significant impact on the Iranian diaspora community in the UK. We also note that whilst the Islamic Centre of England and other cultural and educational centres supported by Iran have legitimate roles supporting the Iranian diaspora community, there are grounds to suggest that they are also being used to promote violent and extremist ideology.

[7] Oral evidence – Home Secretary, 6 July 2023.

- **In the Middle East**: British citizens, particularly dual nationals (since Iran does not recognise dual nationality), face a risk of arbitrary detention – the likelihood of which has increased since the recent protests in Iran. The UK has substantial personnel, security, maritime and commercial interests in the Middle East which are at risk from Iranian hostile activity, along with the threat of terrorism, increased migration and nuclear proliferation. There is also a threat of collateral damage to UK Armed Forces stationed in the region (resulting from misidentification or miscalculation), due to the sizeable number of personnel and their co-location with heavily targeted US forces. One of Iran's key asymmetric capabilities is its extensive ballistic missile programme. It has a large number of short- and medium-range systems which enable it to threaten UK interests – such as deployed forces – throughout the Middle East. This missile capability has been used to target the UK's regional allies and represents a credible threat for Western missile defences. In 2019, Iran almost certainly used missiles and drones to target Saudi Arabia's oil infrastructure, in response to the US policy of 'maximum pressure'. In addition, in 2020 Iran launched a ballistic missile strike against Coalition forces at the Ayn al-Asad airbase in Iraq in response to the US killing of IRGC Quds Force (IRGC-QF) Commander General Qasem Soleimani. Given the volatility of the situation and the possibility for rapid escalation, at some point it could become necessary to evacuate UK nationals in the region. The Committee notes the importance of proper preparation for a possible evacuation. ***: the Government must ensure that it has learnt the lessons from recent evacuation operations such as the withdrawal from Afghanistan.

"The whole toolkit is in play when it comes to Iran."[8]

11. As for the Government's response to this multifaceted threat, the Committee welcomed the increased focus on Iran in the 2023 Integrated Review Refresh. However, it is clear that Government policy on Iran has suffered from a focus on crisis management and has been primarily driven by concerns over Iran's nuclear programme – to the exclusion of other issues. Our External Expert witnesses criticised the Government's approach to Iran as being insufficiently strategic and long-term. 'Fire-fighting' has prevented the Government from developing a real understanding of Iran and – as we have previously noted in relation to Russia and China – 'longer-term' must mean the next 5, 10, 20 years – not 6–12 months.

12. It was also not clear to the Committee that the Government's strategies are aligned – or who is ultimately responsible. As with our previous Inquiries into state threats, the Government appears to over-complicate its structures and strategies: too much resource goes into talking and co-ordinating, at the expense of front-line action. In particular we note that, while there are Iran-specific strategies, we were told that the Government's new Counter-State Threats Strategy is apparently actor-agnostic – addressing state threat activity thematically rather than geographically. While there will be some elements of state threats which are broadly similar – and benefits to be gained from making the UK a hard operating environment, for example – there will be fundamental differences which could be overlooked. The Iranian threat is quite different in many respects, and it is essential that it receives

[8] Oral evidence – Director General MI5, *** June 2023.

sufficient priority and that Russia and China do not crowd out other concerns. On the same grounds, we are concerned that there have been so few National Security Council meetings on Iran.

13. Resourcing on Iran has fluctuated over the past decade, suggesting that the response to the Iranian threat has been short-termist. ***. It is important that resourcing on Iran is consistent with the threat; the Government should take a longer-term view. We also note that MI5 has still not been given the additional funding and resources for which we called in our *Extreme Right-Wing Terrorism* Report.[9] Without a commensurate increase in resources, MI5 cannot be expected to absorb responsibility for an increased range of issues, without other areas of work suffering as a consequence. In this context we particularly commend MI5's work to respond to the rise in the threat of a physical attack by Iran – thwarting at least 15 attempts at murder or kidnap against British nationals or UK-based individuals since the beginning of 2022.

14. In the context of the finite resources allocated to addressing the wide-ranging threat posed by Iran, it is important to factor in the 'force multiplier' effect of the UK's international partnerships. UK, US, *** policy objectives and intelligence requirements are broadly aligned with regard to Iran, and the Agencies' partnerships with their US *** counterparts on the Iranian threat are of critical importance. The *** countries operate with an exceptionally high level of trust. This close collaboration is one of the Agencies' greatest assets: it yields great value and lessens burdens.

15. In terms of the level of understanding of the threat posed by Iran, the Intelligence Community have *** coverage of Iran's capability, *** understanding of its intent, particularly in relation to the ***. This is of the utmost concern given the potential for misunderstanding and miscalculation between Iran and Israel. Whilst the Committee acknowledges that Iran is a hard intelligence target, the Intelligence Community must continue to prioritise improving their understanding of Iran – specifically ***. In terms of the Government, we note the lack of Iran-specific expertise more broadly and that there is seemingly no interest in building a future pipeline of specialists beyond mention in a 'Strategy campaign': as the Committee was told, "*if you have people running policy in the Foreign Office who don't speak a word of Persian, then that is a fat lot of good, to be honest*".[10]

16. The Government does have key policy tools at its disposal which could be used to good effect against the state threat. We welcome the new National Security Act 2023, which will fill previous legislative gaps in tackling state threats. However, other gaps will remain unless the Official Secrets Act 1989 is reformed. The Government now appears to be backtracking on its commitment to Parliament to take this forward: this is of significant concern given the problems with the Official Secrets Acts regime.

17. There are also concerns around the Government's response to Iran's use of militant and terrorist organisations. The Home Office has rightly proscribed several Iran-supported groups assessed to be concerned in terrorism – such as Al-Qaeda, Hamas and Lebanese Hizbollah – but there are increasingly calls for the UK to proscribe the IRGC as a terrorist

[9] *Extreme Right-Wing Terrorism*, HC 459, 13 July 2022.
[10] Oral evidence – 2023.

organisation. We recognise the complexities inherent in a decision as to whether or not to proscribe the IRGC. However, it appears that the Government is paralysed by the legal and practical difficulties around proscription of a state organisation – given that membership of an organisation proscribed in the UK could lead to arrest, conviction and a custodial sentence, which would apply to around a quarter of the Iranian Cabinet. The Government should fully examine whether it would be legally possible and practicable to proscribe the IRGC and, if so, what the arguments are both for and against – and make a full statement to Parliament.

Terminology

When referring to analytical judgements from the Intelligence Community (primarily the Joint Intelligence Organisation and Defence Intelligence), the Report uses particular terminology concerning probability and analytical confidence. Terms such as 'likely', 'unlikely' and 'almost certain' have a specific meaning and associated probability range when used in intelligence assessment. Likewise, 'low', 'medium' and 'high' analytical confidence have precise definitions as to the extent to which an analytical judgement is directly informed by evidence. We provide more detail on the definitions of these terms in the 'UK Intelligence Coverage' chapter.

THE NATIONAL SECURITY THREAT TO THE UK

The Islamic Republic … is a system that is no doubt adversarial, that seeks to preserve its regional influence … at the cost of regional stability. It interferes in its neighbours' affairs; it doesn't respect sovereignty and international law … it is defined by a particularly paranoid world view.

Dr Sanam Vakil, 21 March 2023

THE IRANIAN REGIME

18. Iran is one of the oldest civilisations in the world, tracing its history back to the Achaemenid Empire, founded in 550 BC. However, the Islamic Republic of Iran – as it is now known – was established in 1979 as part of the Iranian Revolution. This was a pivotal moment in Iranian history, as it moved from an absolute monarchy to a partial theocracy, ruled by the Shi'a clergy – a political system which exists to this day.

Shi'a Islam in Iran

Religion is an integral part of Iranian society and was one of the drivers behind the 1979 Revolution. Islam in Iran, as in the rest of the world, is separated into two main sects, Sunni and Shi'a, which hold different beliefs, traditions and rulings. Whilst Iran's Muslims were predominantly Sunni up until the 16th century, in 1501 the Safavid Empire imposed a form of Shi'a Islam in Iran and, over the next few hundred years, Shi'a Islam became "*deeply entrenched in the cultural, intellectual and political life of Iran*".[11] Learned men of religion – the 'Ulema' (i.e. Shi'a clerics) – developed a prominent role in Iranian society, from arbitrators in legal disputes to important figures of social and political authority.

19. The leader of the Iranian Revolution, Ayatollah Khomeini – a senior Shi'a Islamic cleric in Iran – developed a theory of Islamic government called '*velayat-e faqih*' ('guardianship of the Islamic jurist'). This maintained that secular governments are illegitimate and that religious clerics should rule, with the supreme clerical leader providing guardianship over the nation.

20. This became the founding principle of the post-Revolution regime and forms the backbone of modern Iranian society, where the organs of a modern republic – a legislature, executive and judiciary – exist within a religious clerical system, ruled by the Supreme Leader. Professor Ali Ansari, Professor of Iranian History, University of St Andrews, described it to the Committee as a "*dual system of government … between the revolutionary and the republic*[an] *organs of state*".[12]

Iranian leadership and wider security architecture

The Supreme Leader

21. The Supreme Leader wields tremendous power. Professor Ansari summarised this as: "*The Supreme Leader … is answerable to God and … has the final say on anything that is done*".[13] The Supreme Leader is the ultimate decision-maker, with all regime factions devoted to him and maintaining the Shi'a Islamic system of government. He sets the direction of foreign and domestic policy, maintains overall control of intelligence operations, and

[11] *Revolutionary Iran*, Michael Axworthy, 2013.

[12] Oral evidence – Professor Ali Ansari, 9 March 2023.

[13] Oral evidence – Professor Ali Ansari, 9 March 2023.

wields strong influence over key regime appointments, including candidates for the Presidency and key posts in the President's Cabinet (including intelligence and security roles). In terms of the threat posed by Iran to the UK and its interests, the Ayatollah is therefore key.

22. Ayatollah Khomeini became Iran's first Supreme Leader in 1979. It is not an elected position nor is it time-limited: he consequently held it until his death in 1989. The current Supreme Leader, Ayatollah Ali Hosseini Khamenei, was subsequently appointed. He is now one of the longest-serving leaders in the Middle East.

23. Ayatollah Khamenei represents the traditional 'hard-line' strand of Iranian politics, focused on preserving the revolutionary identity of the state. This includes maintaining the system of Islamic governance first established by Ayatollah Khomeini and retaining the clear suspicion around relations with the West.

The President

24. Iran's President is the head of the Iranian government, elected by the Iranian people for a four-year term. According to the Intelligence Community, the President is responsible for domestic and economic affairs but has limited influence over security and foreign policy.

25. The President (at the time of our Inquiry),[14] Ebrahim Raisi, was elected in 2021 after holding several senior roles in the Iranian state and has close ties to the security establishment. Like Ayatollah Khamenei, President Raisi is a 'hard-liner' – an ultra-conservative cleric from a faction that espouses populist economics and anti-Western policy. He is reportedly a long-term loyalist of the Supreme Leader. However, the influence and role of the President and the republican organs of state have diminished in recent years, as Professor Ansari told the Committee:

> *the republican organs of state have been weakened pretty dramatically over the last 20 years ... the revolutionary organs ... who are somewhat more opaque, tend to take ... decisions under the auspices of the Supreme Leader ... the Presidency as an agency with any sort of autonomy is finished ... and Raisi, the current President is, to my mind certainly, nothing but a cipher ... you can see that in the voting and how he operates.*[15]

26. The Intelligence Community expressed a similar view, describing the President's role in setting the regime's strategic objectives as "*subsidiary*".[16] President Raisi's election means that the regime is more homogenous and conservative than the previous administration under President Hassan Rouhani, who was widely reported to have been more of a reformist who looked more favourably on engagement with the West and clashed with the Supreme Leader. This consolidation of conservative influence across the regime has probably resulted in greater regime unity on domestic and foreign policy.

[14] As previously noted, the Committee began this Inquiry in August 2021 and concluded its evidence-taking before 7 October 2023.

[15] Oral evidence – Professor Ali Ansari, 9 March 2023.

[16] Oral evidence – JIO, *** June 2023.

27. The increased ideological alignment between the Iranian President and Supreme Leader may mean a loss of moderate voices in Iranian decision-making. The Intelligence Community told the Committee that this could make the regime more susceptible to "*policy missteps*" and increase the possibility that it embraces more "*assertive*" policy positions.[17] The recent protests in Iran reflect the fact that the regime is even more detached from the people of Iran than the previous administration under President Rouhani. With Raisi as President, the regime may act in a more provocative manner with less restraint – given Rouhani believed more strongly in engagement with the West – which, it appears to the Committee, may increase the overarching threat Iran poses to the UK.

The Supreme National Security Council

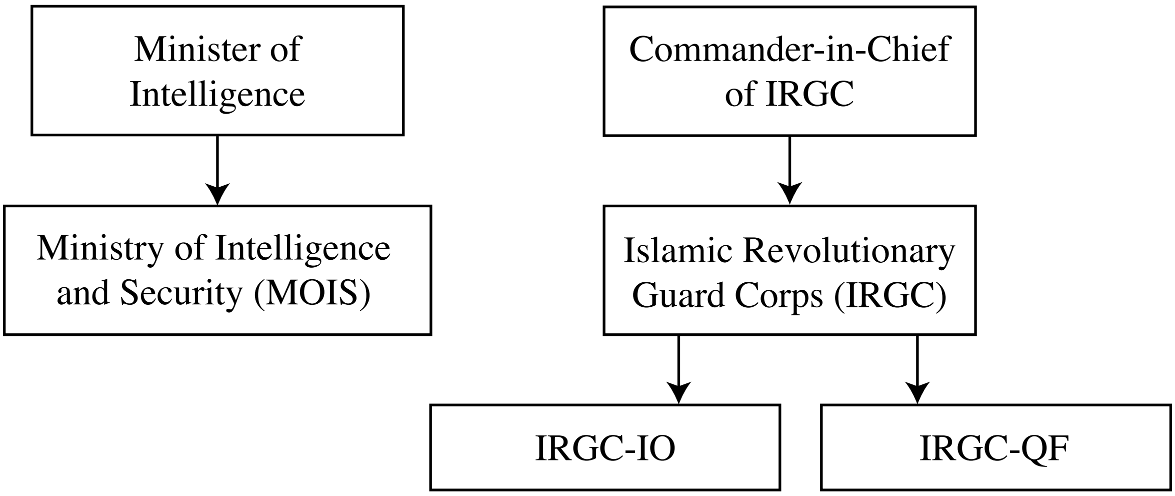
28. Iran's foreign and security policy is led by the Supreme National Security Council (SNSC). The SNSC comprises representatives from the government's different key institutions – both elected and unelected. This includes the President, the Parliamentary Speaker (head of the legislature), the Chief Justice (head of the judiciary), key Ministers (such as Internal, Foreign Affairs and Intelligence), as well as senior representatives from the Armed Forces General Staff, Islamic Revolutionary Guard Corps, the regular army and two representatives nominated by the Supreme Leader. Whilst the President nominally presides over the SNSC, in practice the Supreme Leader controls it (the SNSC is usually co-ordinated by a representative of the Supreme Leader).

29. As part of its role, the SNSC sets the strategic priorities for the Iranian Intelligence Services (IIS), and the Iranian Minister of Intelligence has a permanent seat on it to support the recommendations being made to the Supreme Leader. The SNSC also provides a formal structure for co-operation between the different elements of the IIS, including – for example – consideration of sensitive intelligence operations ***. However, as explored below, the effectiveness of this body to encourage and facilitate such co-operation appears unclear.

Iran's intelligence institutions

30. The IIS consist of two main organisations – the Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps (IRGC) – representing respectively the republican and revolutionary organs of state. Within the IRGC, the main body responsible for intelligence is the IRGC Intelligence Organisation (IRGC-IO), although the IRGC Quds Force (IRGC-QF) – which undertakes foreign military operations – also maintains and operates covert intelligence networks.

[17] Written evidence – HMG, 20 October 2021.


Minister of Intelligence
Ministry of Intelligence and Security (MOIS)
Commander-in-Chief of IRGC
Islamic Revolutionary Guard Corps (IRGC)
IRGC-IO
IRGC-QF

31. The Intelligence Community explained that the IIS exist in an environment of competition with both MOIS and IRGC operating domestically and internationally, including on areas such as counter-espionage and counter-terrorism. For example, MOIS, IRGC-IO and IRGC-QF are all active in monitoring Iranian dissident communities and so, in some cases, could even be monitoring the same targets. Nevertheless, Professor Ansari told the Committee that "*the IRGC are ... dominant ...* [they] *are the ones that ... take the priority ... they get prior access to the assets, they get to do things they can then explain afterwards*".[18]

32. The Intelligence Community did not draw a distinction, explaining that both MOIS and the IRGC pose a significant threat to UK national security. (However, the greatest elements of the Iranian threat would presumably derive from the counter-intelligence, counter-terrorism and foreign intelligence work of both organisations.)

33. Director General MI5 told the Committee that: "***". (HMG works *** to prevent Iran from posting undeclared intelligence officers *** in the UK.) The IIS *** they do retain agent networks, including organised criminal groups, which conduct activity outside of Iran on behalf of the Iranian state. These agents are then managed by Iranian intelligence officers ***.

34. In relation to the extent of control that the Iranian leadership exerts over the IIS and the level of their autonomy, Sir Richard Dalton – former UK Ambassador to Iran – told the Committee:

> *my guess is that on major policy initiatives and on major intelligence actions,* [the level of central control] *... is pretty tight ...* [but there is also a] *tendency to try and bring good things to the regime, to your superiors, and that is a force for ill-discipline: you cannot be absolutely sure, for example, whether threats against people resident in the UK have actually been authorised at a very high level.*[19]

[18] Oral evidence – Professor Ali Ansari, 9 March 2023.

[19] Oral evidence – Sir Richard Dalton, 9 March 2023.

35. The Intelligence Community agreed, explaining that, whilst the IIS operate within a general framework, sometimes consulting others, it appears there is still a certain level of autonomy. The Intelligence Community told us that "***".[20] It appears to the Committee that this level of autonomy, together with the overlapping responsibilities and fierce competition within the IIS, increases the risk of unmanaged escalation and contributes to a less predictable, more dangerous threat.

Ministry of Intelligence and Security

36. MOIS is Iran's main civilian intelligence organisation, with personnel numbers in the low tens of thousands ***. It was formally established in 1984 and took over several intelligence organisations which had been set up after the Iranian Revolution.[21] The Minister of Intelligence (i.e. the head of MOIS) is appointed by the President, but the appointment is subject to the approval of the Supreme Leader. The Intelligence Minister (at the time of our Inquiry) is Esmail Khatib, an Iranian cleric who has held the position since 2021 and reportedly has significant experience working in the IIS.

37. MOIS is one of the (if not the) largest intelligence services in the Middle East, with a network of overseas stations that will house both personnel whose presence is declared to the local authorities along with officers who are undeclared. It has a remit to collect intelligence both internally and overseas in support of Iran's strategic objectives, including via cyber and human espionage. It also conducts counter-espionage investigations, counter-terrorism work and hostile operations against dissidents overseas.

38. In 2012, the US government designated MOIS as a terrorist organisation for its support to terrorist groups, including Hamas and Al-Qaeda. The US also accused MOIS of supporting the Syrian regime's suppression of domestic protests and perpetrating human rights abuses against the Iranian people, including beatings, prolonged interrogations, coerced confessions (particularly of political prisoners) and detention without charge. A decade later, the US government sanctioned the Iranian Minister of Intelligence for MOIS's engagement in malicious cyber operations against the US and its allies. The European Union (EU) and the UK have also applied sanctions against individuals linked to MOIS in recent years, in response to human rights abuses and lethal operations conducted against dissidents.

The Islamic Revolutionary Guard Corps

39. The IRGC was established shortly after the Iranian Revolution in 1979 to safeguard the newly established Islamic Republic from perceived enemies at home and abroad and to protect the principles of the post-revolutionary constitution. The IRGC is a paramilitary body which is answerable to the Supreme Leader and – whilst smaller than the Iranian military[22] – comprises personnel in the low hundreds of thousands *** and has its own army, navy and air force. It is headed by a Commander-in-Chief.

[20] Oral evidence – JIO, *** June 2023.

[21] Academic Michael Axworthy explains that the foundations of the organisation are rooted in SAVAK, the secret security organisation that existed before the Iranian Revolution under the Iranian monarchy. (*Revolutionary Iran*, Michael Axworthy, 2013.)

[22] Iran's military reportedly consists of over 400,000 troops in addition to reserves. (*Iran Military Power*, US Defense Intelligence Agency, August 2019.)

40. The IRGC has become a "*major military, political, and economic force*" in Iran and reportedly controls around a third of Iran's economy.[23] It is involved in many of Iran's key military operations, including – for example – patrolling the strategically important Strait of Hormuz (through which approximately 30% of the world's oil supply passes). It also helps to maintain public order, controlling the voluntary militia, the Basij Resistance Force, which has been used to suppress domestic dissent.

41. The IRGC plays an important role in shaping and implementing Iran's foreign policy and security objectives. Whilst the IRGC operates across the world, it is particularly active in the Middle East, where it manages the majority of Iran's relationships with militant and terrorist groups. As such, in leaked footage in 2021, Iran's then Foreign Minister, Javad Zarif, complained that he had "*zero*" influence over Iran's foreign policy due to the influence of the IRGC and the then IRGC-QF Commander, General Qasem Soleimani.[24]

42. The IRGC has been proscribed by the US, but not by the UK or EU. We consider proscription in the Response section of this Report.

IRGC Intelligence Organisation

43. According to the US Defense Intelligence Agency (DIA), IRGC-IO was established in 2009, strengthening the IRGC's involvement in intelligence work. IRGC-IO is Iran's primary military intelligence organisation, which has become increasingly prominent since its establishment and probably has personnel numbers in the low tens of thousands ***. Like MOIS, it has a remit for collecting intelligence both internally and overseas, conducting counter-intelligence operations within Iran and undertaking 'special' operations, including the assassination of Iranian dissidents.[25] Together with the rest of the IRGC, it is responsible for identifying, and protecting the Islamic Republic from, all threats.

44. Whilst the chain of command is complex, the Intelligence Community told the Committee that the head of IRGC-IO reports to the Commander-in-Chief of the IRGC and – as representing one of the main revolutionary arms of the Iranian state – the IRGC-IO head ***.

45. The UK and US governments have repeatedly sanctioned the IRGC and its senior leaders in connection with a range of issues, including Iran's nuclear programme, regional instability and the suppression of recent internal protests. The US has also sanctioned the head of IRGC-IO, Mohammad Kazemi. The US government stated that IRGC-IO is "*one of the regime's most brutal security services with a long record of internal repression*" and that it had recently broadened its scope, to be responsible for "*thwarting perceived political subversion, coordinating and managing the repression of protests, surveilling and throttling the use of the internet and arresting dissidents*".[26]

[23] 'Profile: Iran's Revolutionary Guards', BBC, 3 January 2020.

[24] 'In Leaked Recording, Iran's Zarif Criticises Guards' Influence in Diplomacy', Reuters, 26 April 2021.

[25] According to the US Department of the Treasury, the IRGC-IO has also attempted to assassinate journalists and Israeli nationals in Istanbul. ('Treasury Designates Iranian Regime Operatives Involved in Assassination Plots in the United States and Abroad', US Treasury Website, 1 June 2023.)

[26] 'Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship', US Treasury Department, 26 October 2022.

IRGC Quds Force

46. IRGC-QF is the branch of the IRGC responsible for undertaking covert foreign operations, including maintaining Iran's relations with allied militant and terrorist groups in the Middle East. It has around 5,000 to 15,000 personnel.[27] As part of this role, IRGC-QF maintains and operates intelligence networks around the world. It appears that these intelligence networks undertake surveillance of foreign targets (such as Iranian dissidents, Jewish and Israeli interests), recruitment, interference and influence operations, and lethal operations overseas *** (although we were concerned to learn ***).[28]

Competition within the Iranian Intelligence Services

47. Both the Intelligence Community and our External Experts made clear that there is significant competition within the Iranian security architecture. This applies to the Iranian system as a whole as well as its intelligence organisations. The JIO described the Iranian system as "*complex and fractured* ... [with] *all sorts of feuding and different power centres competing and jostling for position*".[29] The JIO also told the Committee that this fragmented nature presented a challenge to the Intelligence Community's understanding.

48. With regard to the IIS specifically, Professor Anoush Ehteshami – Professor of International Relations, Durham University – explained that the creation of IRGC-IO had led to a duplication in structure, with MOIS and IRGC creating their "*own interrogation centres, their own officers, their own training*". He noted that "*there is a lot of inter-agency competition and it is partly ideological ... but also it is partly about resources*".[30]

49. The significant overlap between the remits of the different IIS organisations has resulted in fierce competition, tension and disagreements. For example, MOIS and IRGC-IO have ***. The Foreign Secretary told the Committee that the level of infighting and competition means that the IIS are "*rather fragmented*" and that "*there are competing power bases ... we slip ... into the, I think, incorrect assessment that they speak with one voice and they think with one mind*".[31]

50. It appears that there are a number of factors contributing to this lack of collaborative ethos within the IIS, potentially including the different identities of each organisation, individual ways of working, a desire to protect their own responsibilities and information, and a competitive desire to be the primary intelligence organisation.

51. Nonetheless, despite the factionalism within the IIS, they can clearly work together (including practical co-operation and shared areas of responsibility, for example ***). It is likely that the relations between the different organisations fluctuate over time, driven in part by perceived usefulness and recent operational success, with different levels of experience, capability and tradecraft existing within each organisation. MI5 explained that the operating

[27] 'Islamic Revolutionary Guard Corps', Counter Terrorism Guide, National Counterterrorism Centre, Office of the US Director of National Intelligence, March 2022.

[28] ***.

[29] Oral evidence – JIO, *** June 2023.

[30] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

[31] Oral evidence – Foreign Secretary, 6 July 2023.

environment is a significant factor. For example, IRGC-QF is likely to have had more experience in conflict zones and MOIS is likely to be more experienced in less violent environments.

52. In theory, there are formal structures to facilitate co-operation within the IIS at a senior level. This includes the SNSC, which sets the overarching strategic priorities for the IIS, and the Intelligence Coordination Committee, which aims to co-ordinate operational activity. It is highly likely that senior figures within the IIS recognise the benefits of co-operation, motivated by a desire to increase effectiveness and value for money, and that MOIS and the IRGC have a pragmatic relationship, using each other's resources ***. However, ***. For example, it is not unusual for there to be an Iranian operation *** which complicates how the UK Government should respond.

53. It is clear that factionalism within the IIS is a "*mixed blessing*" in terms of the threat to the UK.[32] On the one hand, the lack of co-operation presumably undermines the strategic effectiveness of the IIS. On the other hand, it may sometimes make the Intelligence Community's response more challenging, ***, if the different organisations within the IIS are competing with one another.

54. It is a realistic possibility that co-operation and capability-sharing within the IIS will continue to develop. For example, ***. This could increase the effectiveness of the IIS and their geographical reach, which may then increase the threat they pose to the UK.

55. However, we were told by the Intelligence Community that co-operation within the IIS – such as in the Middle East *** – is unlikely to affect UK national security significantly. Even if co-operation within the IIS increases, the Intelligence Community told us that this would *** as it is unlikely that the IIS's objectives in respect of the UK would change. Whilst the Committee recognises that the level of Iranian intent is integral to understanding the overall threat to the UK and to UK interests in the Middle East, it was surprised by this assessment. Even if the IIS's objectives do not change, it appears logical that increased co-operation and capability-sharing would raise the Iranian threat to the UK and would therefore require a commensurate response. However, in response, the Intelligence Community explained that *** – and increased co-operation would not necessarily increase *** – they do not consider that the threat would rise significantly. We consider the overall threat to the UK later in this Report.

A. The foundation of the Islamic Republic of Iran in 1979 was a pivotal moment in Iranian history as it moved from an absolute monarchy to a partial theocracy, ruled by the Shi'a clergy.

B. The Supreme Leader of Iran wields tremendous power – he is the ultimate decision-maker, setting the direction of Iranian foreign and domestic policy. In terms of the threat posed by Iran to the UK and its interests, the Supreme Leader is therefore key.

[32] Oral evidence – ***, *** June 2023.

C. The Iranian threat appears to have increased following the election of Ebrahim Raisi as President, who is more ideologically aligned with the Supreme Leader than his predecessor. This means the regime may act in a more provocative manner with less restraint.

D. The organisations within the Iranian Intelligence Services – primarily the Ministry of Intelligence and Security and the Islamic Revolutionary Guard Corps, representing the republican and revolutionary organs of state – have overlapping remits, which results in fierce competition, tension and disagreement. Whilst the Iranian Intelligence Services operate within a general framework, it appears there is still a certain level of autonomy. Activity may therefore not always be effectively co-ordinated nor centrally authorised.

E. The Committee considers that the relative autonomy of, and factionalism within, the Iranian Intelligence Services increase the risk of unmanaged escalation and contribute to a worrying unpredictability around the Iranian threat to the UK and UK interests in the Middle East. However, increased co-operation and capability-sharing within the Iranian Intelligence Services could also raise the Iranian threat.

OBJECTIVES OF THE IRANIAN STATE

Overarching objectives

56. Whilst the Intelligence Community observed that Iran is an "*inherently unpredictable actor*",[33] it does nevertheless have several consistent overarching objectives. The State's primary aim is to ensure the survival and security of the Islamic Republic: this objective fundamentally determines how Iran acts, and therefore the threat it represents to the UK and its interests. As the Foreign Secretary told the Committee: "*regime survival is absolutely the top priority for the* [Iranian] *regime; everything else is subordinate to that*".[34]

57. Linked to this primary objective, in evidence to this Inquiry we were told that Iran has three key regional aims which – given the UK's interests in the Middle East and the propensity for Iran to project threat beyond the region – clearly affect the UK:

- to be a leading regional power;
- to contain perceived US and Western influence and hostility; and
- to protect Shi'a communities and holy sites.

58. Our External Expert witnesses noted that it is debatable whether Iran's objectives reflect a 'defensive' stance – focused on deterrence – or an 'offensive' perspective, focused on a desire to be an important and influential regional power. Sir Richard Dalton suggested that the Iranian regime's objectives are in fact "*both defensive and aggressive*", with both elements driving Iranian intent.[35]

59. Our witnesses were clear that Iran is "*fundamentally a rational actor*";[36] however, it does not always appear to act in a coherent or strategic way[37] and is prone to misunderstanding actions that others take. This means that, whilst its overarching strategic intent may be relatively well understood, its actions – for example, its operations affecting the UK – might not be so coherently and clearly aligned. As the Joint Intelligence Committee (JIC) Chair told the Committee, the possibility of Iran and the UK misunderstanding each other "*can lead to things which may look irrational to people who are not following closely what is happening*".[38]

[33] Written evidence – HMG, 20 October 2021.

[34] Oral evidence – Foreign Secretary, 6 July 2023.

[35] Oral evidence – Sir Richard Dalton, 9 March 2023.

[36] Oral evidence – ***, *** June 2023.

[37] ***

[38] Oral evidence – JIO, *** June 2023.

What motivates Iran?

60. Iran's acute historical sense of vulnerability and its belief that it can rely only on itself for its security has shaped its key objectives and wider foreign policy. There are several other drivers for its objectives, including:

- a history of perceived foreign interference in Iran;
- Iran's revolutionary 'anti-imperialist' ideology;
- Iran's historical sense of regional importance;
- Israel and the West's military superiority;
- Iran's fear of Western encirclement; and
- in particular, the formative experience of the Iran–Iraq War.

Iran–Iraq War (1980–1988)

Starting just after the Iranian Revolution (1979), Iran's experience of the Iran–Iraq War has an "*important place in the Iranian psyche*".[39] As Professor Ehteshami described, the war "*shaped* [the Iranian] *world view on so many levels*".[40]

Whilst the figures are hard to verify, Iran reportedly suffered at least a million casualties in the war (and at least 300,000 died). The war decimated Iran's economy and infrastructure, costing as much as US$645 billion. Many of those who fought in the war – such as Islamic Revolutionary Guard Corps (IRGC) officers – hold senior positions in the Iranian regime.

The academic Michael Axworthy explained that for many Iranians, the successful defence of Iran from Saddam Hussein's invasion is a matter of pride, reflecting a shift in the perception of its history from one of "*foreign interference and foreign domination* ... [to a country which had] *set up its own government by its own efforts, had rejected foreign meddling and foreign threats, had defended itself for eight years despite great suffering against tough odds*".[41]

The war fostered a feeling of increased isolationism, insecurity and strategic solitude amongst the leaders of the Iranian regime, and a sense that Iran was surrounded by enemies, with no natural allies to guarantee its security – particularly as Western and most Arab states supported Saddam Hussein's efforts to contain Iran's Revolution. As Professor Ehteshami told us: "[the Iranians] *saw that they were completely alone when aggression took place ... they felt they were being punished for the Revolution*".[42]

[39] *Revolutionary Iran*, Michael Axworthy, 2013.
[40] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.
[41] *Revolutionary Iran*, Michael Axworthy, 2013.
[42] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

The Intelligence Community explained that the big lesson that the Iranian state took from the Iran–Iraq War was that "*when the chips are down, people will support anybody, including Saddam Hussein, rather than Iran and therefore we* [Iran] *have to have the means of protecting our country in our own hands ... we need to have hard power to protect Iran*".[43]

This experience also served to foster the Iranian regime's "*deep distrust of international law and institutions*",[44] particularly given the perceived reluctance of the United Nations (UN) to intervene in the war.

(i) Survival of the regime

61. As noted already, the regime's overarching priority is to maintain and protect the Islamic Republic. This – directly or indirectly – shapes all state policy, as the Intelligence Community explained:

> *The overriding objective of the Iranian regime is to preserve the Islamic Republic. That is the mission of the IRGC ...* [and] *the Supreme Leader ... and of course that means it is not simply a matter of the physical safety of Iran, it is also preserving the regime, including its religious roots and its overall ethos, and in that respect Iran regards itself as being surrounded by dangerous enemies who wish to achieve regime change.*[45]

62. This view was consistent with that of our External Expert witnesses. Sir Richard Dalton described regime survival as the "*predominant characteristic in the mindset of the rulers of Iran*".[46] Dr Sanam Vakil, Director, Middle East and North Africa Programme, Chatham House, agreed, stating that "*the Islamic Republic is driven, above all, by its need for security and stability* [with Iran's leadership] *... looking not only to preserve the Islamic Republic but preserve their place in the Islamic Republic*".[47]

63. This overarching priority completely underpins the regime's other domestic and foreign policy objectives. It provides the driver for the security apparatus's efforts to stifle domestic and international criticism. It also explains the development of a nuclear programme and the aspiration to become a leading regional power.

64. According to our External Experts, it also means that the Iranian leadership is "*much more of a flexible, pragmatic ... regime in order to survive, rather than an ideological rigid structure*".[48] It is driven more by opportunism than ideology. For example, Sir Richard Dalton described the Iranian regime's "*transactional nature of doing business bilaterally*

[43] Oral evidence – JIO, *** June 2023.
[44] *Iran's ISIS Policy*, Chatham House, January 2015.
[45] Oral evidence – JIO, *** June 2023.
[46] Oral evidence – Sir Richard Dalton, 9 March 2023.
[47] Oral evidence – Dr Sanam Vakil, 21 March 2023.
[48] Oral evidence – Dr Sanam Vakil, 21 March 2023.

with countries … they will help you if you help them".[49] This flexible, pragmatic, opportunistic approach is also reflected in Iran's relationship with other states and actors that are either ideologically opposed to them (such as Al-Qaeda) or with whom they share a turbulent history (such as Russia).

(ii) Aspirations to be a leading regional power

65. The Intelligence Community told the Committee that it is highly likely that Iran aspires to be a leading power in the region, capable of deterring and withstanding threats from key regional rivals such as Israel and Saudi Arabia. Several of our External Expert witnesses agreed. Professor Ansari suggested that "*the strategic goal of most of the Iranian states in the modern era has been ... great power status*",[50] and Professor Ehteshami noted that Iran increasingly thinks about its "*sphere of influence*".[51]

66. Iran's historical sense of its regional importance is a key driver behind this objective. Our External Experts referred to the Iranian perception of being an ancient and great civilisation rather than just a state. Sir Richard Dalton stated that this translates into an "*intense pride and nationalism ...* [a] *desire for power in the region and a desire to influence what happens in neighbouring countries*".[52]

67. In addition to this more 'aggressive' desire to expand regional influence, Iran's aspiration to be a leading regional power is also linked to more 'defensive' motivations. These are driven by the Iranian regime's belief that Western powers have continually sought to interfere in Iranian affairs going back to the 19th century, concern around being surrounded by better-equipped adversaries, and the need to deter adversaries from attacking Iran (drivers, at least partly, borne of Iran's experience of the Iran–Iraq War).

(iii) Containing perceived Western influence and hostility

68. Whilst Iran's regional objective to contain perceived Western influence and hostility is particularly aimed at the US, Israel and Saudi Arabia, it is clearly also directed towards the UK. This desire to resist the West is also a key pillar of regime legitimacy, motivated by Iran's heightened fear of being encircled by militarily superior Western and regional adversaries. The Intelligence Community explained:

> *when they look to the west, they see Iraq, a country which was invaded by the Americans and was the source of the great patriotic war for Iran in the late 1980s ... to the east they see* [Afghanistan] *with an extreme form of* [Sunni] *government, which they also regard as posing a potential threat to them ... to the south, they see a range of Gulf monarchies and states who they regard as being fundamentally hostile to their interests and to the north, they see a Caucasus which is unstable and where, with some governments, such as Azerbaijan, they have a very difficult relationship. So there is that sense of feeling encircled,*

[49] Oral evidence – Sir Richard Dalton, 9 March 2023.
[50] Oral evidence – Professor Ali Ansari, 9 March 2023.
[51] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.
[52] Oral evidence – Sir Richard Dalton, 9 March 2023.

> *and then over the horizon you have the United States in particular exerting influence into the region, a country which they regard as being fundamentally determined to topple the Iranian regime ... and then also Israel ...* [whom] *they see as posing a significant threat to their interests.*[53]

69. This fear has strengthened over the last few years due to several geopolitical developments, including: the US killing of IRGC Quds Force (IRGC-QF) Commander General Qasem Soleimani; Israel's attacks on Iranian nuclear facilities and oil shipments; and the normalisation of relations between Israel and several Gulf states (known as the 'Abraham Accords').

70. Nevertheless, at the time of writing, it appears highly likely that Iran wants to avoid a full-scale conflict, aiming instead to contain its main adversaries. As Sir Richard Dalton explained, Iran wishes to "*keep the United States at bay ... they want to challenge the United States and show strength in order to do that but they want to avoid inter-state war. They know they would come off worst*".[54] Similarly, he noted that whilst Iran maintains an ideological, religion-based hostility to Israel, the fear of causing an extended conflict within Iran's borders means that thus far there has been relatively little retaliation to Israeli attacks on Iranian assets.

71. Professor Ehteshami described this deterrence approach as a policy of 'strategic depth': avoiding direct extended conflict with superior conventional powers – such as Israel – by creating buffer areas of influence, and ensuring Iran does not fight battles within its own borders. He told the Committee:

> *That is why Syria ... matters to them. That is why open access from Iranian territory to the Mediterranean matters to them. It is all about not just* [the] *sphere of influence but about strategic depth, that we* [Iran] *can do all of our deterring and fighting somewhere else so that our weaknesses are not exposed and we play into our strengths.*[55]

72. Despite Iran's wish to avoid a full inter-state conflict, the Committee was told that, where possible, Iran favours proportionality in relation to conflict, responding in a similar way to which it perceives it has been targeted. In other words, it seeks to maintain 'escalation dominance', always aiming to be in a position in which it is able to escalate hostilities – as that acts as a deterrent to its opponents.[56] It believes that its adversaries would otherwise exploit any perceived weaknesses which could act to undermine domestic support for the regime. As the JIC Chair explained:

[53] Oral evidence – JIO, *** June 2023.

[54] Oral evidence – Sir Richard Dalton, 9 March 2023.

[55] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

[56] Oral evidence – ***, *** June 2023.

> *Iran thinks that it protects itself by what we would describe ... as 'forward defence'.*[57] *They believe they have to be aggressive, that they cannot show weakness, because that would be exploited and therefore any provocation against Iran must be answered, partly so they show strength to their own people but partly to the outside world.*[58]

SIS agreed:

> *What is always true of the Iranians is that, if we do something to them which they regard as antagonistic, they will bite back ... you always have to know that if you up the ante, the Iranians, who have a very high risk threshold, will try and do it.*[59]

73. However, a symmetrical response to conflict is not always achievable or pragmatic – particularly given the military superiority of some of Iran's adversaries. Iran – driven by its isolation and technological inferiority – has therefore focused on the development of niche conventional and 'asymmetric'[60] capabilities as well as a regional network of aligned militant and terrorist organisations in order to deter potential aggressors.

(iv) Protection of Shi'a communities and sites across the region

74. Iran is a Shi'a-majority state in a region of largely Sunni-majority countries and, as such, the Iranian state is a "*self-declared defender of Shi'a causes*" (particularly since the Iranian Revolution of 1979), helping to correct what it perceives as the subordination of the Shi'a community. Iran has therefore supported demands for political reform in Bahrain (a state with a Shi'a majority and Sunni ruling monarchy), and criticised Saudi Arabia for its treatment of its Shi'a minority.[61]

75. This helps to explain Iran's attempts to defeat Sunni extremism, most notably its fight against the terrorist organisation, the 'Islamic State', when it conquered swathes of territory in neighbouring Iraq in 2014. Nevertheless, as noted above, Iran's actions appear to be motivated not only by religious ideology but also by geopolitical pragmatism and the overriding objective of maintaining the safety and security of the regime. This demonstrates why it fought Islamic State – representing a serious threat at its borders – whilst at the same time maintaining a relationship with other Sunni extremist groups, such as Al-Qaeda.

[57] Iran's concept of 'forward defence' has been discussed in open source commentary – for example, 'Treading a Fine Line: Iran and the Israel-Gaza War', RUSI Commentary, 30 October 2023; 'Iran's Influence in the Middle East', House of Commons Library Research Briefing, 14 April 2023.

[58] Oral evidence – JIO, *** June 2023.

[59] Oral evidence – SIS, *** June 2023.

[60] The adoption of an asymmetrical warfare strategy refers to the use of unconventional tactics such as attacking an enemy's weak points in unexpected ways.

[61] 'The Rise of Iran as a Regional Power: Shia Empowerment and Its Limits', *NATO Review*, 24 February 2016.

76. The importance of religion as a motivator in Iran is therefore a complex question. As the JIC Chair explained:

> *I personally think it is outdated to think of Iran as a theocracy. It is much closer to a 'securitocracy' than it is to a theocracy. Religion is a very important binding factor ... which provides motivation through the Supreme Leader and that sense of Shi'a identity which is extremely important to the Islamic Republic but it is not the primary motivator of what they do.*[62]

(v) Ideological opposition to Israel

77. Iran's fierce opposition to Israel is an important part of the Iranian regime's identity. It regards Israel as its "*nemesis*" and it is a topic on which it is continually focused.[63] As Professor Ehteshami noted:

> *anti-Zionism has now become part of their DNA ... it is partly because it was one of the Revolution's narratives ... they have continued to maintain this line that ... the state of Israel founded on Zionism, does not have a legitimacy in the region ...* [and whilst former Iranian Presidents] *Rafsanjani* [and] ... *Khatami tried to dilute it ... the Leader, for his own reasons and identity is so wedded to this that it is almost impossible for anyone ... as far as he is alive, to challenge this as a modus operandi of the regime.*[64]

78. Iran's animosity towards Israel is also motivated by the need to maintain the safety and security of the regime and contain regional adversaries. As the JIC Chair said, whilst religion is a factor in this animosity, it is "*much more because they perceive Israel as a country which is set on toppling the Islamic Republic, or ... is prepared to defend its own territory in a way which Iran will find aggressive*".[65]

(vi) Economic growth

79. The Intelligence Community consider the Iranian economy to represent a "*headache to be managed rather than an imminent threat to regime survival*".[66] Dr Vakil agreed, asserting that Iran is not driven by economic objectives: "*I don't think that there are economic objectives involved for the Islamic Republic; there are only security objectives*".[67]

80. Nevertheless, the domestic economy is clearly of importance to Iran. The combined effect of international sanctions and years of economic mismanagement have harmed the Iranian economy. As a result, some Iranian politicians believe it needs at least some sanctions relief to safeguard the regime's long-term future, even though they may not believe that Iran's weak economy is an immediate threat to the regime.

[62] Oral evidence – JIO, *** June 2023.
[63] Oral evidence – JIO, *** June 2023.
[64] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.
[65] Oral evidence – JIO, *** June 2023.
[66] Written evidence – HMG, 20 October 2021.
[67] Oral evidence – Dr Sanam Vakil, 21 March 2023.

81. Driven by its desire for sanctions relief, it is highly likely in the medium-to-long term that the Iranian regime will seek to boost domestic production and strengthen trade ties with neighbours and eastern countries such as India and China. Sir Richard Dalton said that due to Iran's inability to trade in Europe, Iran has "*turned increasingly to people willing to trade with them who tend to be further east. So development of those strategic relationships, those comprehensive agreements with Russia and China, are front and centre*".[68]

82. We questioned whether Iran's economy has any bearing on the threat posed by Iran to the UK. The Intelligence Community told the Committee that there was "*no visible direct link*" as Iran's main priority is the survival of the regime.[69] Nonetheless, it appears that there may still be an indirect connection. For example, in relation to the recent domestic protests in Iran, following the death in police custody of Mahsa Amini, the JIC Chair noted: "*some of the unrest which we have seen in Iran over the last 12 months has partly an economic angle to it and that has actually stimulated more aggression by the Iranian security services*".[70]

F. The Iranian regime's fundamental objective is to ensure the survival and security of the Islamic Republic: it has an acute historical sense of vulnerability. This shapes – directly or indirectly – all of its actions. This focus on survival means Iran is a pragmatic actor, often driven more by opportunism than ideology (more 'securitocracy' than theocracy).

G. The Iranian regime has three key regional aims: to be a leading regional power; to contain perceived US and Western influence and hostility; and to protect Shi'a communities and holy sites.

H. Whilst Iran favours proportionality in relation to conflict, this is not always achievable or pragmatic as it wants to avoid a full-scale war. It therefore has focused on the development of 'asymmetric' capabilities and a network of aligned militant and terrorist organisations across the Middle East to spread influence and deter potential aggressors.

I. Iran also maintains a fierce ideological, religion-based hostility to Israel, regarding it as its arch enemy. The Supreme Leader is so wedded to this narrative – from the Revolution – that it is now part of the Iranian regime's DNA.

J. Iran is motivated by both defensive and offensive considerations. Much of Iran's foreign policy – and the threat it represents to the UK – is borne of a historical sense of its regional importance, a fear of encirclement by better-equipped Western adversaries, a history of perceived foreign interference in Iran, and the formative experience of the Iran–Iraq War.

K. While Iran is fundamentally a rational actor, it does not always appear to act in a coherent way and is prone to misunderstanding actions that others take.

[68] Oral evidence – Sir Richard Dalton, 9 March 2023.

[69] Oral evidence – JIO, *** June 2023.

[70] Oral evidence – JIO, *** June 2023.

IRAN AND THE UK

83. The UK and Iran have a complex relationship, with a series of bilateral disputes over the last 40 years.

UK–Iran relations

The following events and issues have played a key role in UK–Iran relations from 1979:

1970s

UK International Military Services (IMS) tank debt: In the mid-1970s, the UK sold over 1,500 tanks to Iran, who paid c.£600 million in advance. By the time of the 1979 Revolution, after which the UK broke off diplomatic relations, only 185 tanks had been delivered. This served as a point of contention until 2022, when the UK paid £400 million to Iran, which has been linked in the media to the release of British-Iranian dual nationals from imprisonment in Iran.

1980s

Fatwa against Sir Salman Rushdie: In 1989, the then Supreme Leader of Iran, Ayatollah Khomeini, issued a *fatwa* (Islamic religious decree) ordering Muslims to kill Sir Salman Rushdie, a British citizen, in retaliation for his authorship of *The Satanic Verses*. After this, diplomatic ties between the UK and Iran were not fully restored until 1998. In 2022, Rushdie was stabbed at a literary event in the US.

2000s

Allied invasions of Afghanistan and Iraq: With the NATO invasion of Afghanistan in 2001 and the US–UK invasion of Iraq in 2003, British forces came into close proximity with Iran (and holy Shi'a sites in Iraq). Iran also detained British Royal Navy sailors in 2004 and 2007, and supported Shi'a militia attacks on British forces in Iraq.

Election of President Mahmoud Ahmadinejad: Iranian President Ahmadinejad's election in 2005 worsened the relationship between Iran and the international community. In the context of the seemingly fraudulent 2009 Iranian elections and associated protests in Iran, President Ahmadinejad accused the UK (and BBC Persian) for interfering in Iran's internal affairs.

2010s

Storming of the British Embassy in Tehran: In response to UK and EU sanctions against Iran in 2011 (which were imposed after President Ahmadinejad disengaged from nuclear negotiations), Iranian students and militia stormed the British Embassy in Tehran, which the UK then closed along with the Iranian Embassy in London.

Election of President Rouhani and the Joint Comprehensive Plan of Action (JCPOA): The election of the more moderate Iranian President Rouhani in 2013 paved the way for improved relations with Iran, including the 2015 JCPOA nuclear agreement, after which formal UK–Iran diplomatic relations were restored. As will be explored later in this Report, the JCPOA provided partial sanctions relief for Iran in return for restrictions on its nuclear programme. However, relations with the West (including the UK) deteriorated rapidly when the US withdrew from the JCPOA and reimposed sanctions in 2018.

Detention of Nazanin Zaghari-Ratcliffe: Nazanin Zaghari-Ratcliffe, a British-Iranian dual national, was detained in Tehran in 2016 on charges of espionage and leading a foreign-linked hostile network. Her eventual release from prison in 2022 has been widely linked in the media to the UK paying Iran its £400 million IMS tank debt.

2020s

Killing of General Qasem Soleimani: In January 2020, General Soleimani, the head of Islamic Revolutionary Guard Corps Quds Force (IRGC-QF), was killed in Iraq by a US drone strike, following which the UK Ambassador to Iran was summoned to the Foreign Ministry in Tehran (Iran reportedly viewed the UK as an accomplice due to its statements following the attack which highlighted the aggressive threat posed by IRGC-QF). In response to the worsening relations and events – including Iran shooting down a Ukraine International Airlines civilian aircraft, killing 176 people – the Foreign, Commonwealth and Development Office (FCDO) strengthened its travel advice for both Iran and Iraq; the Ministry of Defence changed the readiness of UK forces in the region; and the Department for Transport issued guidance on the threat to British shipping.

Execution of Alireza Akbari: In January 2023, UK–Iran relations worsened further after Iran executed Alireza Akbari, a British-Iranian dual national accused of espionage. In response, the UK temporarily recalled its ambassador in Tehran and imposed sanctions on Iran's Prosecutor-General.

Human rights and 2022–23 protests: The UK's longstanding criticism of the human rights situation in Iran has increased since widespread protests broke out in Iran in September 2022 (after Mahsa Amini was beaten and died in police custody in Tehran). Thousands of Iranians have been detained and hundreds killed in the regime's violent suppression of the protests. In response, the UK (alongside others) has sanctioned associated Iranian organisations and individuals, including the Deputy Prosecutor-General, the Commander of the Iranian Army Ground Force, the Deputy Commander of the IRGC in Tehran, the Basij Resistance Force, and the Deputy Commander of the Basij Resistance Force.

How does Iran perceive the UK?

84. Views of the UK vary across the Iranian regime and public, and this complex picture was reflected in the different opinions provided by our External Experts. Professor Ansari stated:

> *the perception of Britain in the Iranian imagination ... is quite a mixed one and in some ways quite a powerful one ... there is a deep admiration for the way in which* [the UK] *handles* [its] *politics ...* [a] *feeling that Britain understands how to operate politically* [which] *... has deep historical roots ... and it is one that I think you can see also in the level of interest that Iranians have for coming here for education, for medical treatment ...* [and] *'Perfidious Albion'*[71] *is in some ways quite admired.*[72]

85. Sir Richard Dalton provided a different view, stating emphatically that Iran has an "*intensely negative view of* [the UK]". He explained that Iran thinks that:

> *We* [the UK] *weren't able to carry out our own obligations under the JCPOA* [nuclear deal] *to normalise trade and finance ... We are not a significant influence on the United States or the Europeans anymore. We are close allies of the Arab states on the other side of the Gulf* [i.e. Iran's adversaries] ... [and] *I think they despise us for our evident double standards, along with the United States, on human rights questions.*

He continued:

> *where Britain is concerned, the Iranians feel that they haven't got anything serious from us; so what is there to lose? It is not just scapegoating; it is what is there to lose in their relationship with the UK if* [Iran] [...] *try* [for example] *extraterritorial violence against their political opponents?*[73]

86. However, in general, Iran's leadership perceives the UK as a significant adversary, and one which poses a military and intelligence threat in the Middle East. It believes that the UK is opposed to the Iranian regime's values and aims and – as part of the West – is seeking regime change in Iran. Iran therefore perceives the UK to be a potential threat to the security of the Iranian regime (although witnesses have suggested that the UK would sit behind the US, Israel and Saudi Arabia in any priority list). This perception is partly influenced by the Iranian image of the UK as a 'cunning fox', a metaphor which is rooted in historical narrative and literature. As the JIC Chair summarised:

> *the United Kingdom has an astonishing potency in their mind ... there is a deep suspicion* [of the UK] *for historical reasons as well as relatively contemporary reasons.*[74]

[71] 'Perfidious Albion' is the idea that Britain is considered treacherous in international affairs, reportedly coined in the 18th century.

[72] Oral evidence – Professor Ali Ansari, 9 March 2023.

[73] Oral evidence – Sir Richard Dalton, 9 March 2023.

[74] Oral evidence – JIO, *** June 2023.

Iran's strategic objectives towards the UK

87. Iran's main strategic objectives[75] towards the UK are (in no particular order):

- to undermine UK relations with the US and Israel;
- to weaken the UK's security relationships in the Middle East;
- to reduce the UK's military presence in the Middle East; and
- to silence the UK's criticism of Iran (on issues such as human rights).

88. These clearly support Iran's overarching objective of protecting the regime as well as containing the West, one of its key regional objectives. When summarising Iran's approach to the UK, the Intelligence Community noted that Iran also intends to protect Shi'a communities worldwide and represents a significant threat to Israeli and Jewish entities – although Director General MI5 made clear that such matters "*pale into comparative insignificance alongside the central obsession of maintaining the regime*".[76]

89. Director General MI5 said that this primary objective had a significant effect on the Iranian threat posed to the UK:

> *Survival of the regime itself is still overridingly their number one priority and so the great majority of activity* [in the UK] *that my teams have had to detect and counter over the last few years now has been targeted at their own dissidents,* [... at] *Persian language media organisations, anyone who is perceived as potentially posing a threat to the Supreme Leader and the religiously influenced system that they operate.*[77]

90. The threat posed by Iran is also linked to the state of the bilateral relationship between Iran and the UK. This relationship could change depending on the UK's international engagement as much as UK-specific actions or policy. For example, ***. The Intelligence Community also noted that Iran's approach towards the UK is closely linked to its approach to the US – unsurprising, given the close alignment between the UK and US.

91. In addition, Iran's UK-related objectives will be affected unpredictably by institutional and personal tensions within the Iranian regime. As explored in the previous chapter, there are different factions within the Iranian establishment. It is not a homogenous entity (although its leadership has become more ideologically aligned following the election of President Raisi in 2021).

[75] In addition to its four strategic objectives, from the evidence we received, it appears to the Committee that Iran's tactical objectives in relation to the UK include: to monitor dissident communities in the UK and silence critics of the Iranian regime; to gather information on HMG and the Intelligence Community, in order to protect the Iranian regime and enable Iran to respond; and ***, for example by targeting Israeli and Jewish interests in the UK.

[76] Oral evidence – MI5, *** June 2023.

[77] Oral evidence – MI5, *** June 2023.

Overall threat to the UK

92. The JIC Chair told the Committee that Iran represents a "*very wide-ranging and difficult threat*".[78] SIS described the Iranian Intelligence Services (IIS) as "*highly capable adversaries*"[79] and MI5 said that they are "*sophisticated* ... [and] *regard the UK as a long-term adversary*".[80]

93. The Home Secretary agreed with these assessments, emphasising the severity of the Iranian threat to the UK. She cautioned that "*the Iranian Intelligence Services pose a persistent and sophisticated threat to the United Kingdom and to our interests overseas. We are no doubt a priority for Iran*"[81] – although, as we have noted previously, this will be behind the United States and Israel. Director General MI5 added: "*if the Iranians were to make ... a policy decision to materially increase their focus on the UK, ****".[82]

How does the Iranian threat compare with Russia and China?

94. The Committee reported on the state threats posed by Russia and China in 2020 and 2023 respectively. The Intelligence Community told the Committee that, by comparison, Iran represented one of the leading threats to the UK but of a different nature to Russia and China:

> *Iran has a particular role in the* [Middle East] *region ... but if you think about it more as a threat to the United Kingdom ...* [they] *would be top of the Championship rather than in the Premier League,*[83] *but rising. Russia and China ... have a scale and a capability which Iran cannot match.* [But] *what Iran has, is a risk appetite which is very 'pokey' indeed.*[84]

95. Iran's activity certainly appears less strategic than that of China and Russia. The Home Secretary told us: "*I would describe the nature of the threat as slightly chaotic. It is not as strategic as we have seen from the Chinese and the Russians. There seem to be waves of activities ... rather than a kind of consistent plan*."[85] Director General MI5 agreed, explaining that the IIS "*do not have the scale or some of the strategic aims that in particular we see the Chinese pursuing. So the Chinese and the Russians in their different ways are substantially more strategic ... in terms of the breadth of what they are interested in doing inside the United Kingdom*."[86]

[78] Oral evidence – JIO, *** June 2023.
[79] Oral evidence – SIS, *** June 2023.
[80] Oral evidence – MI5, *** June 2023.
[81] Oral evidence – Home Secretary, 6 July 2023.
[82] Oral evidence – MI5, *** June 2023.
[83] The Premier League and the Championship are the highest and the second-highest leagues in the English football league system.
[84] Oral evidence – JIO, *** June 2023.
[85] Oral evidence – Home Secretary, 6 July 2023.
[86] Oral evidence – MI5, *** June 2023.

96. The number of intelligence officers in the IIS – in the tens of thousands – is also significantly smaller than the Russian and Chinese equivalents, which are in the low hundreds of thousands. Nevertheless, Iran still poses a significant – and broad – threat to the UK, which should not be underestimated. As Director General MI5 told us:

> *The Iranians are quite interesting because they present across all the different forms of threat. They ... do* [some] *political interference in the United Kingdom ... They engage in terrorism; they are a respectable cyber power ... they are kind of there across the full spectrum of the kinds of threats we have to be concerned with.*[87]

97. We consider the various aspects of the threat – including nuclear, physical, espionage, offensive cyber and interference – in the following chapters.

L. Iran and the UK have a complex history. Iran's leadership perceives the UK to be a significant adversary – a 'cunning fox' – opposed to the Iranian regime's values and, as part of the West, to be seeking regime change in Iran. It therefore believes that the UK poses a military and intelligence threat in the Middle East – although witnesses suggested that the UK would sit behind the US, Israel and Saudi Arabia in any priority list.

M. Iran's main strategic objectives towards the UK include: reducing the UK's military presence in the region; undermining the UK's relationships with the US and Israel; weakening the UK's security relationships in the Middle East; and silencing criticism of Iran, either from the UK directly or from those residing in the UK.

N. The threat posed by Iran is also linked to the state of the bilateral relationship between Iran and the UK. This relationship could change depending on the UK's international engagement as much as UK-specific actions or policy. The Intelligence Community also noted that Iran's approach towards the UK is closely linked to its approach to the US – unsurprising given the close alignment between the UK and the US.

O. Whilst Iran's activity appears to be less strategic and on a smaller scale than Russia and China, Iran poses a wide-ranging, persistent and sophisticated threat to UK national security, which should not be underestimated.

[87] Oral evidence – MI5, *** June 2023.

IRAN'S INTERNATIONAL PARTNERSHIPS

98. As previously noted, Iran has an acute sense of its position in the region – including its perceived vulnerability – and this drives its strategy towards its international partnerships. For example, Iran has strengthened its relations with Russia and China in recent years, improving its economic, military, intelligence and diplomatic ties with both countries. Iran has also maintained a strong relationship with Syria – one of the oldest alliances in the Middle East – supporting the Syrian regime in its civil war, which has raged since 2011. Iran also maintains relationships with North Korea, *** and beyond its broader geopolitical partnerships with other states, Iran also maintains relationships with aligned militant and terrorist ('proxy') groups across the Middle East. These are considered at the end of this chapter.

Russia

(i) Overarching relationship

99. Sir Richard Dalton told the Committee that Iran wants to build a "*deep alliance*" with Russia, which is reflected in the "*expected Russian investment in* [Iran's] *oil and gas, the development of the inland overseas transport routes to assist the circumvention of sanctions both against Russia and against Iran, the sales of advanced weaponry into Iran,* [and] *Russian purchases of Iranian weapons*".[88] The Foreign Secretary noted the increasingly close relationship between Russia and Iran, stating: "*it is clear that Russia has chosen its partner of choice in the Middle East and that partner is Iran*".[89] The Government's Integrated Review Refresh of 2023 also voiced concern about this growing co-operation.

100. This development is despite a legacy of distrust and suspicion between the two countries, arising from Russia's historical involvement in Iran and the region. As such, it is driven by political expediency – for example, shared concerns about the United States – rather than a deep historical connection or ideological link. Indeed, Professor Ansari noted that "*of the two countries* [Russia and the UK], *Russia has probably perpetrated much more egregious harm to Iran over the last 150 years and yet, somehow, it turns out to be a sort of an ally at the moment*".[90]

101. The improvement in the relationship can currently be seen in Iran's military support to Russia in Ukraine and previously through their collaboration and intervention in the Syrian Civil War which – according to some academic commentary – the Iranian military viewed as essential for the survival of Syrian President Bashar al-Assad. *** Russia and Iran have a strong mutual military dependence in Syria and a shared intent to defend the Syrian regime. Iran and Russia both also provide significant economic support to Syria – for example, there

[88] Oral evidence – Sir Richard Dalton, 9 March 2023.

[89] Oral evidence – Foreign Secretary, 6 July 2023.

[90] Oral evidence – Professor Ali Ansari, 9 March 2023.

is evidence that Iran has provided crude oil to the Syrian regime and Russia has probably helped the Syrian regime to evade international sanctions, representing Syria's link to the international banking system.[91]

102. Nonetheless, Russia and Iran are still rivals, competing, for example, for economic, military and political influence in Syria (despite their shared intent to defend the Syrian regime). Similarly, whilst they have previously shared objectives in Afghanistan, they hold different positions on other Middle Eastern states such as Israel, Saudi Arabia, Turkey and Yemen. Russia also wants to prevent a nuclear-armed Iran and supported the 2015 Joint Comprehensive Plan of Action (JCPOA) nuclear deal.

(ii) Intelligence co-operation

103. It appears that Iran and Russia share intelligence, with the Iranian Intelligence Services (IIS) and the Russian Intelligence Services (RIS) likely to be co-operating in a number of areas where they have issues of mutual concern or of particular interest to either side.[92] Such co-operation may increase the threat in terms of espionage and tradecraft. Nevertheless, any such collaboration is likely to be limited by the historical distrust between them. The JIC Chair told us: "***."[93]

104. In addition to sharing intelligence, the RIS may help the IIS with capabilities: Russia and Iran signed a defensive cyber co-operation agreement on sharing information and technology in 2021. It is likely that Russia is providing advice and guidance to Iran, helping Iranian cyber actors to refine their approach and using its cyber expertise (reportedly in monitoring and intercept capabilities)[94] with Iran as a relatively cheap tool to promote its own strategic interests in the region. Such co-operation may lead to better security practices.[95]

105. There may also be some co-operation between the IIS and the RIS in relation to interference operations. For example, the disinformation website VeteransToday.com regularly reposts articles from both PressTV (the Iranian state broadcaster's main English-language television channel) and the Russia-linked New Eastern Outlook. It is, however, unclear to what extent this activity reflects strategic co-operation rather than opportunistic recycling of content.

106. It may be that the co-operation between the IIS and the RIS extends to gathering information on HMG. Whilst the IIS would presumably be the junior partner in such a relationship, collaboration of this sort could still result in the IIS becoming more capable and increase the threat posed by the IIS to HMG (including to the Intelligence Community), potentially allowing them to run more effective agent operations and undermine Western intelligence efforts. For example, reporting *** indicated ***.

[91] 'Treasury Sanctions Financial Facilitators and Illicit Drug Traffickers Supporting the Syrian Regime', US Department of the Treasury, 26 March 2024; 'Iran is Still Exporting Oil to Hezbollah and the Assad Regime. It's Using Syrian Ports for Transit', Atlantic Council, 13 March 2023.

[92] ***.

[93] Oral evidence – JIO, *** June 2023.

[94] 'Russia Supplies Iran with Cyber Weapons as Military Cooperation Grows', *Wall Street Journal*, 27 March 2023.

[95] ***.

(iii) Military co-operation

107. Russia has historically been a major supplier of arms to Iran. The end of the UN conventional arms restrictions in 2020 probably provided an opportunity for Iran to upgrade its Russian-manufactured equipment, albeit presumably Iran may have been precluded from procuring major new items by the cost, given Iran's struggling economy. Iran may want a wider defence agreement ***. Russia and Iran have also co-operated on advanced satellites for the last decade – for example, in 2022 Russia launched an Iranian imagery satellite from Kazakhstan. Most notably, however, Russia's invasion of Ukraine has created significant opportunities for further collaboration with Iran.

Russia's invasion of Ukraine and co-operation with Iran

It has been widely reported that Iran has provided weaponry to Russia for use in its invasion of Ukraine – according to the Washington Institute, Iranian drones in particular have become an "*increasingly important weapon for Russia*",[96] which it has used against Ukrainian military and civilian targets.

As such, President Volodymyr Zelenskyy of Ukraine said in January 2023 that Iranian drones launched by the Russian military had been shot down over his country. The US and UK governments have also acknowledged Iran's support to Russia. For example, the US Central Intelligence Agency (CIA) Director publicly said that Russia is likely offering Iran help with its advanced missile programme in exchange for military aid for its war in Ukraine. The UK Foreign Secretary also stated in December 2022 that this co-operation meant that Iran had become "*one of Russia's top military backers*".[97]

When we questioned the Intelligence Community on how Russia's invasion has affected its relationship with Iran, they told the Committee:

> *It certainly has provided a boost to the Iran–Russia relationship. The relationship between Iran and Russia has never been one of deep friendship. It is an alliance of need ... but the fact that Iran has been willing to provide Russia with significant military capability, particularly through the provision of UAVs* [unmanned aerial vehicles] *** *that there has been a general inclination to lean towards each other.*[98]

There are indications that this co-operation also extended to the Russians sharing Western military kit that they have obtained on the battlefield with Iran,[99] which is undoubtedly very useful for the Iranian regime. As the Deputy National Security Adviser (DNSA) concluded, the growing relationship between Russia and Iran – including the exchange of military equipment and technology – is "*incredibly concerning*".[100]

[96] 'What Iran's Drones in Ukraine Mean for the Future of the War', Washington Institute for Near East Policy, 10 November 2022.

[97] 'Iran and Russia "Sordid Deals" Threaten Global Security: Foreign Secretary's Statement', HMG, 9 December 2022.

[98] Oral evidence – JIO, *** June 2023.

[99] ***

[100] Oral evidence – DNSA, *** June 2023.

108. We questioned whether Iran's closer alignment with Russia posed a threat to UK energy interests. The JIC Chair did not think so, telling the Committee:

> **** I would not expect to see evidence that Iran would seek to influence the situation in Ukraine by attacking energy interests in the Gulf.*[101]

China

(i) Overarching relationship

109. Iran has a deep economic relationship with China – indeed, China is Iran's largest trade and economic partner. China reportedly represents "*36 per cent of* [Iran's] *total exports*"[102] and benefits from access to cheap Iranian oil, one of the most significant areas of the Iran–China relationship. Our External Experts explained that Iran's inability to trade with Europe – due to the imposition of Western sanctions – has acted as a driver for Iran to enhance its relationship with China, due to its willingness to trade with Iran:

> *While we isolate Iran, we are literally pushing it towards China. Iran being lost to China has profound implications for regional as well as global balance of power … there is that very powerful economic dimension to it, that if Iran cannot get* [trade] *from Europe any longer, or from the United States, or from Western allies, it will get it for sure from China, and the Chinese are very happy with that.*[103]

110. However, there is more to the relationship than purely economic considerations. Professor Ehteshami explained that Iran and China share similar world views, including their perception of themselves as "*great Asian civilisational powers*", which underpins a desire by each to project their regional and global influence.[104] Their two world views share the primary objective of preserving regime legitimacy, a sense of grievance in relation to past foreign interference, and a suspicion of the West.

111. Iran and China signed a 25-year Comprehensive Strategic Partnership (CSP) in 2021, which – according to media reporting – includes economic, military and cyber security co-operation. The same reporting has suggested that China has agreed to provide Iran with new technology to strengthen its state surveillance infrastructure capable of monitoring landline, mobile and internet communications. Iran also became a member of the Shanghai Cooperation Organisation in May 2023, in which China plays a prominent role, and which aims to enhance political, security and economic engagement between its member states. Despite this co-operation, China will continue to maintain a balance of relationships across the region, including with Iran's adversaries such as Saudi Arabia and Israel.

[101] Oral evidence – JIO, *** June 2023.

[102] 'Iran Exports', *Trading Economics*, accessed on 1 November 2023.

[103] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

[104] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

112. The need to balance these relationships may have led to China sponsoring an agreement between Iran and its key regional adversary, Saudi Arabia, in March 2023. The agreement reportedly provided a plan for re-establishing diplomatic relations over the following months. We questioned the Intelligence Community on the significance of the agreement and whether it could – indirectly – lead to a change in the Iranian threat to the UK. The JIC Chair explained:

> *China saw an opportunity for brokerage and took it. It wasn't a longstanding Chinese ambition which they worked for over years to achieve ... it has reawakened in China a sense of its potential to become an international broker ...* [but] *I am not sure that I can draw a trail of bread crumbs between the threat to the UK and* [this] *Chinese activity.*[105]

(ii) Intelligence co-operation

113. The IIS maintain a relationship with the Chinese Intelligence Services, including with the Chinese Ministry of State Security, and may want to develop the same intelligence relationship as they have with the RIS. For example, ***. A report by the US-China Economic and Security Review Commission referred to media reporting that indicated that "*China and Iran may have conducted high-level cooperation on intelligence matters that dismantled much of the US espionage network in both countries*".[106]

114. China may well share strategically important intelligence with Iran – ***. China could also seek to increase intelligence sharing with Iran on various regional issues; however, the intelligence relationship is probably of less significance compared to the economic relationship. With that said, the CSP may indirectly lead to a closer intelligence relationship.[107]

(iii) Military co-operation

115. China has previously supplied anti-ship cruise missiles to Iran and assisted with small-scale upgrades to fighter aircraft. However, it has sold relatively little weaponry to Iran since the early 2000s and faces fierce competition from Russia. Activity was curtailed by UN sanctions and – in the case of anti-ship cruise missiles – by Iran's successful domestic missile development programme. Iran does, however, appear to rely on China for some key drone components. Under the CSP, military co-operation reportedly includes joint training as well as research and co-operation in Iran and China's respective defence industries.[108] According to the US-China Economic and Security Review Commission, China and Iran maintain modest defence co-operation but that "*despite Iran's signals that it would welcome a more*

[105] Oral evidence – JIO, *** June 2023.

[106] 'China-Iran Relations: A Limited but Enduring Strategic Partnership', US-China Economic and Security Review Commission, 28 June 2021.

[107] ***

[108] 'China and Iran Deal: Much Ado About Nothing?', International Institute for Strategic Studies, 7 April 2021.

formalized defense partnership, China and Iran do not have a military alliance and it is unlikely the two countries will establish one".[109] DI summarised the bilateral defence relationship between Iran and China as: "***".[110]

116. Both Russia and China have, however, collaborated with Iran on space technology. ***. ***, this may well be important for Iran's civilian and military sectors.

North Korea

117. Several of our External Experts referred to the relationship between Iran and North Korea, including North Korea's support for Iran militarily – for example on Iran's ballistic missile programme. Ambassador John Bolton, former United States National Security Adviser, in particular emphasised that:

> *This connection between North Korea and Iran, which we do not fully know about or understand is something that should be in our minds at all times ... we know that the North Koreans have detonated six nuclear devices and that they are working rapidly to develop warheads that they can place on top of ICBMs* [intercontinental ballistic missiles] *and if that information is being shared with Iran – and we just don't know one way or the other – that is a very significant fact.*[111]

118. Ambassador Bolton also noted that Iran and North Korea have developed a relationship as part of their shared determination to maintain the stability of their respective regimes. He said that Iran "*finds natural partnerships with other resistance-based isolated states and this axis of resistance that Iran has built and will probably continue to build, provides a partnership, often times transactional but pragmatically orientated, to help like-minded regimes survive*".[112] Equally, The Rt Hon. the Baroness Ashton of Upholland, former High Representative of the European Union for Foreign Affairs and Security Policy, observed that during high-level diplomatic meetings she had attended in South East Asia, "*it was very very obvious that there was a great closeness between* [Iran and North Korea] *that I found hard to understand and hard to establish exactly what was going on*".[113]

119. The Intelligence Community told the Committee that Iran and North Korea have co-operated economically and militarily. The economic relationship has existed since the 1980s, with North Korea relying on Iran for oil and humanitarian aid. They have also co-operated on arms and technology, primarily because of their mutual isolation from the international community, with the main area of military co-operation being ballistic missiles – Iran having historically used North Korean missile technology as the basis of some of its systems. ***.[114] (We address the question of nuclear co-operation later in the 'Nuclear Programme' chapter.)

[109] 'China-Iran Relations: A Limited but Enduring Strategic Partnership', US-China Economic and Security Review Commission, 28 June 2021.
[110] Oral evidence – DI, *** June 2023.
[111] Oral evidence – Ambassador John Bolton, 21 March 2023.
[112] Oral evidence – Ambassador John Bolton, 21 March 2023.
[113] Oral evidence – Baroness Ashton, 21 March 2023.
[114] Written evidence – DI, 5 July 2023.

Syria

120. As noted above, it is clear that Iran – together with Russia – has provided significant military assistance to the Syrian regime to help it survive the Syrian Civil War. This assistance could include the provision of intelligence monitoring techniques and training. In terms of co-operation between the IIS and the Syrians, SIS told us: "*we would assume, given the investment that Iran has made into Syria, right across its military ***, they will be pretty well plugged in*" – although we note that given the Syrians' predominantly internal focus, that may not have much of an effect on the threat to the UK.[115]

***

121. *** According to the National Cyber Security Centre (NCSC), multiple Iranian *** linked cyber actors – such as *** as it is referred to in the public domain)[116] – subsequently provided assistance, and it is highly likely that they were working ***. It is likely that this included defensive scanning of *** networks, vulnerability scanning of *** networks, and preparations for influence operations ***.

***

122. ***

Aligned militant and terrorist groups in the Middle East

123. Beyond its broader geopolitical partnerships with other states, Iran maintains a network of complex relationships with militant and terrorist groups across the Middle East, with differing levels and types of support. This includes relationships with: broadly religiously aligned Iraqi Shi'a militant groups (SMGs) such as the Badr Organisation, Asaib Ahl Al-Haq and Kata'ib Hizbollah; the Houthis in Yemen; Hizbollah in Lebanon; SMGs in the Gulf; as well as organisations with whom Iran has a pragmatic, transactional relationship despite potentially conflicting religious ideologies, such as Al-Qaeda, the Taliban and Palestinian groups such as Hamas. It maintains these relationships through both the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS), but particularly IRGC Quds Force (IRGC-QF), which provides training, lethal aid, funding and (in some cases) direction to these groups.

Why does Iran support a network of aligned militant and terrorist groups in the Middle East?

124. Iran supports these groups as a key tool for achieving its regional objectives. As the 'Objectives of the Iranian State' chapter explains, Iran's overarching goals – of maintaining the security of the regime, aspiring to become a leading regional power and containing the West – have led to its development of a foreign/military strategy that seeks to expand its regional influence (through developing a continuous land corridor from Iran to the Mediterranean), fight its enemies outside its borders and deter its foreign adversaries from engaging in direct conflict with it.

[115] ***.

[116] It is routine for government and industry to use different names to refer to the same group of cyber actors.

125. This includes developing a doctrine of 'strategic depth' – avoiding direct conflict with superior conventional powers by creating 'buffer' areas of influence, ensuring that Iran does not enter into conflict within its own borders, and developing 'asymmetric capabilities' – using relatively simple but deadly weapons in unexpected ways and employing unconventional tactics to attack an enemy's weak points and deter further attacks.

126. Iran's network of regional militant and terrorist groups provides it with a deniable means of attacking its adversaries – such as UK Armed Forces and the UK's regional allies (as well as regional cities, militaries and trade) – and undermining Western interests in the region with minimal risk of retaliation against Iranian territory. The International Crisis Group refers to this as Iran's 'forward-defence' policy, where it can "*meet its enemies on the battlefield through proxies without direct harm to Iran and its people*". It has also been referred to as an 'Axis of Resistance'.[117]

127. One such example is Iran's significant support to Hamas and Palestinian Islamic Jihad (both of which are Palestinian terrorist groups, proscribed by the UK). This includes weapons, cyber assistance, financial support and potentially advice on public relations and media services. DI assesses that since 2006, Iran has focused on providing Hamas with the expertise and equipment to produce rockets locally and also to improve the group's ability to operate Iranian-made rockets. SIS explained that Iran supports Hamas and Palestinian Islamic Jihad to help counter Israel in addition to other Arab states and that they co-operate due to a shared enmity towards Israel and in spite of their overarching ideological differences.

128. The Intelligence Community told the Committee that Iran's complex network of relationships has produced mixed results. On the one hand, it has helped Iran expand its regional (and global) influence and status, as well as its logistics network. This may have led Iran to believe that this has helped to deter its key adversaries from attacking it directly and contained Western interests and influence. However, these destabilising tactics have not entirely deterred Israeli or US attacks; in fact, they may even have encouraged such attacks and are highly likely to have strengthened Israeli–Gulf alignment.

How much control does Iran maintain over this network?

129. The Iranian regime has varying degrees of control *** over each of the regional militant and terrorist groups with whom it maintains a relationship ***.

130. This was emphasised by our External Experts. Sir Richard Dalton said that: "*I don't think Iran has absolute control of either its partners or its proxies ... you have to look at each individual case ... but, as a general principle, these are not puppets on the end of a string that ends with Ayatollah Khamenei*".[118]

131. This view appears to also be held by some current and former US government officials. For example, the media reported that "[US] *Intelligence officials have calculated that Tehran*

[117] 'Iran's Priorities in a Turbulent Middle East', International Crisis Group, 13 April 2018.

[118] Oral evidence – Sir Richard Dalton, 23 March 2023.

does not have full control over its proxy groups in the Middle East."[119] NPR, a US broadcaster, reported a former US intelligence official saying that "*the control will vary by group and by actor*"[120] and *The Guardian* reported a former US diplomat as saying "*I am not sure they have as much control over some of their proxies as they wanted.*"[121]

132. When the Committee questioned the Intelligence Community, the JIC Chair explained: ***.[122] Like Iran, most – but not all – of the groups belong to some form of Shi'a Islam but they are often also nationalist and have their own interests, unwilling to serve Iranian interests where they diverge from their own. The Chief of SIS told us:

> *It is extraordinarily complex ... ***, and I think since the death of* [IRGC-QF Commander] *Qasem Soleimani, ***.*[123]

133. As Iran does not retain overall control, its support for such groups – providing funding, training and weaponry – risks an escalation of aggression in the region. We heard from witnesses that it is possible that Iranian-supported militant and terrorist groups will take unilateral action, believing – perhaps mistakenly – that they are following the broad parameters of Iranian strategic direction. This risk of miscalculation is likely to increase should the Iranian regime make public statements which are inconsistent with its internal foreign policy objective.

Which Iranian-aligned militant and terrorist groups pose the biggest threat to the UK?

134. Several militant and terrorist groups in the Middle East which have a relationship with, and to varying degrees receive support from, Iran – such as Kata'ib Hizbollah in Iraq and Al-Qaeda – have demonstrated both the capability and intent to threaten UK interests. Other notable groups, such as Lebanese Hizbollah, do not appear to have the intent – given their regional focus and publicly stated objectives – but retain the capability to target UK interests. The threat posed by these groups is examined below.[124]

(i) Kata'ib Hizbollah and other Iraqi Shi'a militant groups

135. Iran has exerted long-term influence over many Iraqi Shi'a militant groups (SMGs) since the early days of the Iranian Revolution, but the degree of Iranian influence, loyalty and control over each group varies significantly. Iran increased its support for these groups following the invasion of Iraq in 2003, with the primary aim of using them to force the

[119] 'US Intelligence Officials Estimate Tehran Does Not Have Full Control of Its Proxy Groups', Politico, 2 January 2024.

[120] 'The US is Demanding Iran Rein in Its Proxy Groups. Is That Actually Possible?', NPR, 7 February 2024.

[121] 'As Middle East Crisis Grows, Does Iran Have Control of Its Proxy Forces?', *The Guardian*, 6 January 2024.

[122] Oral evidence – JIO, *** June 2023.

[123] Oral evidence – SIS, *** June 2023.

[124] As stated in paragraph 3 of this Report, the Committee concluded its evidence-taking before Hamas's terrorist attack on Israel on 7 October 2023. This Report does not therefore consider the attack or any of the subsequent events. It also does not assess whether there has been a change in the Iranian threat to the UK or UK interests as a result.

withdrawal of Western forces. As such, over the last two decades, many of these groups have attacked US personnel, enabled and directed by Iran. For example, Asaib Ahl Al-Haq – which has been supported by Iran – was reportedly responsible for claiming over 6,000 attacks on US and Coalition forces between 2006 and 2010 (and was designated a terrorist organisation by the US government in 2020). Iran's relationships with Iraqi SMGs are managed primarily through IRGC-QF, which provides varying levels of training, weaponry and non-lethal equipment, significantly improving their capability.

136. Whilst these SMGs mainly pose a threat to US interests, the co-location of US and UK Armed Forces represents a significant collateral threat to UK forces, due to the risk of misidentification and miscalculation. For example, in 2020, it is highly likely that Iraqi SMGs were responsible for the targeting of diplomatic Coalition convoys in the 'Green Zone' (the area of Baghdad in which Western assets are situated). In addition, in 2021, there was a large-scale drone attack on Coalition forces in Syria, with Iraqi SMGs almost certainly responsible.

Kata'ib Hizbollah

Kata'ib Hizbollah is a prominent Iraqi SMG which acts as a 'proxy' organisation on behalf of Iran. It is highly likely that IRGC-QF was involved in Kata'ib Hizbollah's creation in 2007 to oppose the presence of Coalition Armed Forces in Iraq following the invasion in 2003. It is likely to have received significantly more training from Iran than other Iraqi militant groups.

It is likely that Kata'ib Hizbollah is the Iraqi militant group most willing to conduct attacks against Western interests in Iraq (and capable of carrying out the most effective attacks). Kata'ib Hizbollah has frequently conducted attacks on Coalition forces and the US designated it as a terrorist group in 2009. According to the Intelligence Community, *** its most likely method of attack is using Improvised Explosive Devices and projectiles against Coalition convoys.

(ii) Al-Qaeda

137. As has been reported in both intelligence and media reporting, the strategic direction of Al-Qaeda (AQ) – which was proscribed as a terrorist group by the UK in 2001 – is led by the 'Hattin Committee', a group of AQ senior leaders located in Iran. In 2020, it was reported that AQ's second-in-command, Abu Muhammad al-Masri, had been killed in Iran, with the then US Secretary of State Mike Pompeo subsequently accusing Iran of allowing AQ to establish an Iranian base (which has been repeatedly denied by the Iranian regime).

138. In addition to Iranian *** support, the ability of the Hattin Committee to stay in Iran – while not without challenge – has provided it with protection from Western counter-terrorism activity and a relatively secure operating environment.

139. The positive relationship between Iran, a theocratic Shi'a regime, and AQ, an extremist Sunni terrorist group is – on the surface – surprising. However, as was explored in the

'Objectives of the Iranian State' chapter, the regime's priority is to survive, and this makes it flexible and transactional, driven more by opportunism than ideology. As the Chief of SIS told us, the Iranian regime has been "*extremely pragmatic for many years in terms of the partners it will enlist, if they are prepared to work against its common enemies in the shape of the United States, the West, Israel in particular*".[125]

140. Whilst it is possible that there is some operational co-operation between AQ and Iran, the Intelligence Community assess that ***. Whilst the full relationship ***, it is highly likely that AQ will remain wary of co-operating too closely with Iran and that the relationship will remain pragmatic and transactional, because of the deep mutual distrust.

141. Whilst AQ rarely mentions the UK specifically as a target, it is almost certain that it views it as such and that AQ maintains the intent and capability to target UK interests. Each AQ global affiliate also represents a threat to Western interests in their own respective region. The permissive operating environment in Iran could have helped AQ to increase its coherence as an organisation and strengthen its capability against the West. However, it is more likely that the Hattin Committee's presence in Iran has had mixed results: on the one hand, it may well have helped AQ to survive as a network; however, any reputational costs incurred by the relationship, coupled with what may be practical challenges around operating in Iran, may well have hampered the influence and control the Hattin Committee has over its affiliates.

142. We asked the Intelligence Community how AQ's presence in Iran has affected the threat to the UK and were told that, on the one hand, being based in Iran has allowed AQ to retain some oversight of franchises internationally, creating a complex intelligence landscape, as Iran is a less accessible environment for the West than other parts of the Middle East – which, in turn, may have increased the AQ threat. Conversely, ***. As SIS told the Committee, it is therefore a "*very complex judgement*".[126]

143. Nonetheless, we noted that the Intelligence Community had previously judged that an AQ attack in the West with input from ***. We note that AQ publicly claimed an attack on a US Naval Air station in Florida in December 2019 – supposedly the last successful AQ operation in the West. ***

(iii) Lebanese Hizbollah

144. Formed in 1982 with Iranian support to combat the Israeli invasion of Lebanon, Lebanese Hizbollah is Iran's most trusted junior partner, central to Iran's objective to deter Israel from attacking it. As part of the Lebanese political system, Lebanese Hizbollah is very well resourced and operates almost at a state level. The UK proscribed the entirety of Lebanese Hizbollah in 2019 (and had previously proscribed its international wing – the External Security Organisation – and its military wing in 2001 and 2008 respectively).

145. Iran provides Lebanese Hizbollah with extensive funding, weaponry, non-lethal aid and training. It is highly likely that Iran has provided Lebanese Hizbollah with access to a

[125] Oral evidence – SIS, *** June 2023.
[126] Oral evidence – SIS, *** June 2023.

broad spectrum of weaponry, which has increased its capability and access to resources. It has access to drones (receiving extensive support from Iran to develop this capability), a significant number of rockets, and possesses the greatest cyber capability of all terrorist groups worldwide. Evidence suggested that Lebanese Hizbollah is able to conduct numerous and concurrent international operations and very probably has sleeper cells[127] and operatives *** in several countries across the globe, including possibly the UK.[128] (MI5 subsequently told the Committee in 2023 that ***.) Its agents very probably conduct activity including money laundering and contingency attack planning in case such capability is required by Lebanese Hizbollah or Iran.

146. Given its regional focus and publicly stated objectives, it appears unlikely that Lebanese Hizbollah has the intent to target directly *** UK interests worldwide. Nevertheless, it would appear to have both the capability and intent to attack Western interests (it is highly likely that the targeting of US and Israeli interests – such as in the Middle East – is of a greater priority than the targeting of UK interests). As with Iraqi SMGs, it is possible that UK nationals could be affected – either due to misidentification or as collateral damage – by any attack targeting US interests, due to the co-location of UK and US assets.

147. The Committee was concerned to learn that there is ***. Given their historical capabilities,[129] there is a possibility that Lebanese Hizbollah has the capability to conduct an attack on UK territory if it chose to do so (***). In the event that Lebanese Hizbollah did conduct an attack here, US or Israeli interests would represent the most attractive targets.

148. When we questioned the Intelligence Community, MI5 told the Committee:

> *We do know about their presence here, we have looked at that through our investigative work *** we will look at any specific strands of threat that we see. The intelligence picture, as with all of this, is not perfect *** the amount of lethal threat we are seeing from the Iranian intelligence sources more directly.*[130]

We return to the issue of *** in the Response section of this Report.

P. Iran's acute sense of its position in the region – including its perceived vulnerability – drives its strategy towards its international partnerships.

Q. Iran wants to build a deep alliance with Russia, and the relationship is becoming increasingly close – despite a legacy of distrust and suspicion – particularly since the Russian invasion of Ukraine, with Iran providing weaponry to Russia. The relationship is driven by political expediency rather than ideological connection. It appears likely that their intelligence services co-operate and share intelligence.

[127] A 'sleeper cell' is a group of covert agents who are inactive for a long period, waiting to be activated.

[128] As is explored later in this Report, in 2015 a Lebanese Hizbollah sleeper cell was linked to the stockpiling of explosive precursor material in the UK as part of its contingency planning should Iran or Lebanese Hizbollah judge that an attack was necessary.

[129] The 2015 campaign, noted above at footnote 128, is covered later in this Report.

[130] Oral evidence – MI5, *** June 2023.

R. China is Iran’s largest trade and economic partner, and they share a world view driven by preserving regime legitimacy, a sense of grievance in relation to past foreign interference, and a suspicion of the West. Whilst there may well be intelligence exchanges between the two countries, the intelligence relationship is probably of less significance than the economic relationship.

S. Iran has developed a network of complex relationships with militant and terrorist groups across the Middle East to which it provides differing levels and types of support. It maintains these relationships through both the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security, but particularly the IRGC Quds Force, which provides training, lethal aid, funding and, in some cases, direction to these groups. This network is part of Iran’s doctrine of ‘strategic depth’, ensuring that it does not enter into conflict with superior conventional powers within its own borders. It provides Iran with a deniable means of threatening its adversaries – such as UK Armed Forces and the UK’s regional allies – and undermining Western interests in the region with minimal risk of retaliation against Iranian territory.

T. The varying level of control that Iran exercises over its network of aligned militant and terrorist groups – and the different interests represented within it – exacerbates the unpredictability of the Iranian-backed threat in the Middle East and risks an escalation of aggression in the region.

U. The transactional arrangement between Iran and the senior leadership of Al-Qaeda (AQ) is concerning. Being based in Iran has allowed AQ to retain some oversight of franchises internationally, creating a complex intelligence landscape, as Iran is a less accessible environment for the West than other parts of the Middle East – which, in turn, may have increased the AQ threat.

THE THREAT: PHYSICAL ATTACKS

149. This chapter refers to the physical threat posed to UK nationals or those resident in the UK by Iran – notably the threat of a physical attack such as kidnap, forced repatriation, assassination or terror attack. (The physical threat to UK nationals based in the Middle East is covered later in 'The Threat to UK Interests in the Middle East' chapter and harassment is covered in the 'Interference' chapter.)

150. While threats from cyber-attacks or nuclear weapons may perhaps be more high-profile, HSG told the Committee that the threat of physical attack on individuals in the UK is now "*the greatest level of threat we currently face from Iran*".[131]

151. A stark illustration of this issue is the adoption by Iran of kidnap and assassination as state policy. In 2016, the Intelligence Community assessed that Iran used assassination as an instrument of state policy and had the risk appetite to assassinate someone in the UK, albeit only in extreme circumstances. By the time of our Inquiry, it was clear that Iran represented one of the highest kidnap and assassination state threats to the UK (***). Director General MI5 noted: "*we do see the Iranians having a higher risk appetite *** most of the time*". This means that Iran probably has the intent to kidnap a UK-based Iranian dissident (by way of a forced repatriation) – and may seek to assassinate a UK-based Iranian dissident.

Iranian intent to carry out physical hostile activity

Focus on the dissident community

152. Monitoring and silencing UK-based opponents of the Iranian regime is one of Iran's primary tactical objectives in relation to the UK. The focus of the Iranian physical threat is therefore directed against Iranian dissidents including, potentially, assassination (how Iran prioritises the dissidents it targets and its precise risk appetite for targeting a dissident in the UK *** later in the Report). There is also an increased threat against Jewish and Israeli interests in the UK.

153. Targeting dissidents is a high priority for both the Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps (IRGC) (***). Again, this shows the direct link between the level of threat in the UK and Iran's objective of maintaining the security of the regime – which means challenging anyone whom it perceives as acting in opposition to it. Iran almost certainly views these hostile activities as a legitimate part of its pursuit of its wider defence and foreign policy objectives. The JIC Chair explained:

> *the Iranian* [physical] *threat ... manifests itself in the United Kingdom, principally against people who the Iranian regime believes pose a threat of some sort to the regime itself, which is, after all, the main area of safeguarding for the Islamic Republic ... Iran is not thinking about this in territorial terms,*

[131] Oral evidence – HSG, 21 June 2023.

> *it is heavily focused on what they regard as the threat to the Islamic Republic of Iran.*[132]

154. Iran's intent to undertake such operations against UK-based dissidents and organisations critical of the regime is therefore almost certainly not viewed by Iran as constituting a direct attack on the UK; from the perspective of the Iranian government, it is not about the UK – rather, it perceives attacks on dissidents as necessary to defend Iran, regardless of where these critics of the regime are based. The UK is therefore almost a 'collateral' in Iran's fierce desire to remove its perceived enemies. As Director General HSG summarised, "*what we see here is the sort of prosecution of what they see as internal matters on UK soil*".[133] This was demonstrated in 2018 when the Dutch government expelled two Iranian diplomats following the assassination of two Iranian dissidents in the Netherlands. In response, MOIS strongly denied the claims, emphasising that the two dissidents were terrorists, and criticising the Dutch for having provided a safe haven.

155. Professor Ansari emphasised the severity of this threat. He told the Committee:

> *I know* [of] *a number of* [people] *... who have come under quite serious threats ... it is pretty intolerable ... that we have to suffer a situation where* [we] *have to, on very short notice, be taken to safe houses because of realistic threats being issued ... I have been quite stunned myself ... at the level or the intensity of this and what is going on and the amount of care that some people who are quite voluble in their criticism of the regime have had to take.*[134]

156. As the threat is specifically targeted at those individuals perceived to be opposed to the Iranian regime, the Iranian threat to the wider population in the UK is judged to be significantly lower. The Intelligence Community assessed that there was only a remote chance that Iran would conduct a physical attack in the UK against a member of the general public, beyond those whom they specifically target (the triggers for Iran to conduct attacks on UK territory and *** activities and intent ***). It is unlikely, for example, that the Iranian regime (***) would sanction terror attacks against the general public in the UK unless there was a significant escalation in tensions between Iran and the UK, which – according to Iran – might justify the consequences of any operation.

157. Equally, whilst the Iranian regime has sanctioned several UK Parliamentarians whom it believes are hostile to the regime, the Intelligence Community told the Committee that it is highly unlikely that those individuals face an increased risk of physical threat.

158. Nonetheless, there clearly remains a risk of collateral damage to the wider UK population in the event of an attack: Iran has demonstrated a willingness to conduct attacks using methodologies which would be highly likely to result in significant collateral damage to individuals in the area (for example, the attempted bombing of the Iranian opposition group Mujahideen-e-Khalq (MEK) conference in Paris). *** the Iranian Intelligence Services

[132] Oral evidence – JIO, *** June 2023.

[133] Oral evidence – HSG, 6 July 2023.

[134] Oral evidence – Professor Ali Ansari, 23 March 2023.

(IIS) have been linked to preparations for a wider physical attack in the UK in case the Iranian regime determines that such an attack is required (the impacts of which would potentially not be limited to the dissident community).

Increase in physical threat

159. Whilst the Iranian physical threat by the IIS to UK-based individuals whom Iran perceives to be a threat to the regime has existed for some time, it became clear during our Inquiry that it has significantly increased recently both in pace and with regard to the number of threats: in 2022, the Intelligence Community raised their assessment of this threat ***. The Home Secretary told us: "*the Iranians have demonstrated a high appetite for risk and a high appetite for using sophisticated measures and there has been a sharp increase in the last six to 12 months …* [of] *that risk appetite … demonstrated by the IIS*".[135] HSG noted: "*the Iranian … physical threat in the UK is now on a comparable level with Russia*".[136]

160. That sharp increase in the physical threat represents the biggest change over the last 12 to 18 months in the overall Iranian threat to the UK. The Home Secretary and MI5 explained that this increase is driven mostly by the insecurity of the Iranian regime, which has been fuelled by the recent protests in Iran – demonstrating how the domestic situation in Iran can indirectly affect the Iranian threat to the UK. In particular, MI5 told the Committee that it has seen persistent targeting of Iranian media organisations operating in the UK, primarily Iran International. BBC Persian and Manoto TV – which are broadcast from the UK – are also prominent targets, as they are viewed by Iran as "*deeply undermining of the Iranian regime*".[137]

Protests in Iran[138]

In September 2022, Mahsa Amini, an Iranian-Kurdish woman, was arrested and beaten by Iran's morality police for her alleged failure to comply with the country's Islamic dress code. She died in police custody three days later. Amini's death triggered waves of protests for over 100 days in Iran. The Iranian government's response – which included the use of force against, and detention of, protesters as well as suppression of the internet (which involved parts of the IIS) – was condemned internationally, including by the UK.

161. The increased Iranian physical threat has been reflected in public statements made by the Intelligence Community. This includes the Annual Threat Assessment of November 2022 provided by Director General MI5 in which he said: "*Iran projects threat to the UK directly, through its aggressive intelligence services. At its sharpest this includes ambitions to kidnap or even kill British or UK-based individuals perceived as enemies of the regime. We have seen at least ten such potential threats since January alone*".[139]

[135] Oral evidence – Home Secretary, 6 July 2023.

[136] Oral evidence – HSG, 21 June 2023.

[137] Oral evidence – MI5, *** June 2023.

[138] 'Iran Protests 2022: Human Rights and International Response', House of Commons Library, 26 May 2023.

[139] 'Annual Threat Assessment', Director General MI5, 16 November 2022.

162. The Intelligence Community told the Committee during our Inquiry that this has increased further, to at least 15 such threats (since the beginning of 2022), of which the majority have "*related to media organisations but there is also* [the] *threat to dissidents associated with political parties that are seen as in opposition to the Iranian regime and also occasionally to Jewish individuals of prominence as well*".[140]

163. This is clearly a significant national security threat to the UK. It is not surprising that, when we asked the Home Secretary which national security threat kept her awake at night, she said:

> *I have got increasing concern about the pace of increase relating to the Iranian threat in the last six months or so. That is, in particular,* [in] *relation to the Iranian Intelligence Services' attempts ... to assassinate, lure and kidnap UK-based individuals who they perceive to be a threat to the stability of the Iranian regime, and that has been a longstanding threat but ... the impact has been markedly increasing over recent months. That has taken up increasing resource from MI5, Counter Terrorism Policing and other law enforcement and security agencies ... it is going in only one direction; I don't see that abating.*[141]

Iranian capability in the UK

164. Iran's capability to undertake hostile operations overseas is amplified by the global networks of the IIS and its cyber capabilities: notably, Iranian cyber espionage operations against travel and financial companies are judged to have provided bulk data on travel patterns which may have been used to support physical operations against dissidents. As will be explored further in subsequent chapters, the Iranians also exploit social media and conduct other hostile cyber activity to access technology belonging to targets. GCHQ told the Committee:

> *It* [is] *highly likely that Iran has used its cyber capabilities in intelligence gathering against dissidents in the UK ...* [they] *have the capability to exploit social media and open source information to help them gather information about their targets. We are also aware of them using very specific capabilities targeting the individuals, for example spear-phishing in order to gain access to targets' accounts but also potentially deploying malicious software onto the targets' phones. So they do use their cyber capabilities, both IRGC and MOIS, against dissidents. We judge that to be in support of the targeting they are doing anyway, so it is not necessarily to identify individuals but, where they know they have a target of interest, they will use their cyber capabilities as a way of gathering further intelligence on them to inform some of those other operations.*[142]

165. Previous hostile operations have demonstrated that the IIS are persistent with their targeting and have a long memory: they can be willing to wait for a long time for the opportunity to target those seen to act in opposition to the Iranian regime. However, there are

[140] Oral evidence – MI5, *** June 2023.

[141] Oral evidence – Home Secretary, 6 July 2023.

[142] Oral evidence – GCHQ, *** June 2023.

sometimes indicators of potential Iranian interest in an individual – for example, an Interpol Red Notice (i.e. a request to law enforcement worldwide to locate and arrest an individual pending extradition) against members of Iranian dissident groups for terrorism-related offences.

Potential actors: the Iranian Intelligence Services

166. During this Inquiry, we received evidence suggesting that both MOIS and the IRGC undertake such hostile operations outside of Iran (***). It is very probable that MOIS and the IRGC have a pragmatic relationship, using each other's resources in operations overseas, *** (subject to the limitations on co-operation examined previously in the Report).

167. MI5 told the Committee that:

> *the successful assassinations ... in Europe in previous years were largely MOIS-orchestrated but recently quite a lot of IRGC threat has been projected towards the UK, and *** both in parallel and *** a co-ordinated effort across the Iranian system to conduct operations against* [the media organisation] *Iran International in particular.*[143]

Potential actors: third-party agents

168. Despite the IIS's involvement in hostile physical threat operations, ***, and the UK remains a difficult operating environment for them. They often rely on other organisations to undertake such hostile activity on their behalf. MI5 told the Committee:

> *The way in which they conduct this activity is to use proxy groups which can be proxy organisations that are associated with the Iranian regime but also criminal groups and occasionally Islamist extremists as well and they are prepared to use a very wide range of individuals to conduct operational activity on their behalf because it is deniable, because they ***. So proxy groups is the easiest way for them to try and project the threat into the UK.*[144]

169. Organised criminal networks have been used by the IIS to conduct successful hostile operations in Europe, such as assassinations. Sometimes these criminals are recruited as operatives who themselves are not aware of the purpose of their activity. This includes using drug smuggling networks, such as the group run by the Iranian narcotics trafficker and IIS agent, Naji Sharifizindashti, who was previously based in Turkey. His network has been linked to the 2019 murder of an Iranian dissident in Istanbul on behalf of Iran (***).

170. We questioned the Home Secretary as to whether the use of organised criminal groups to conduct hostile activity on behalf of Iran could spread to the UK. She gave a stark response:

> *Because of the range of methodologies, vectors, that the Iranians are deploying, I do believe that we will see more lethal activity and ... they are increasingly*

[143] Oral evidence – MI5, *** June 2023.

[144] Oral evidence – MI5, *** June 2023.

> *using proxies, violent thuggish proxies ... these kind of very elusive, quite sophisticated, very brutal European-wide gangs who don't obviously have a connection or a sympathy or a natural allegiance to the Iranian regime and those global criminal networks are conducting assassinations around Europe and that is how I believe it may well evolve here. So I can see the kind of outcome being more serious.*[145]

171. At present, MI5 assesses that there are currently *** between the IIS and UK-based organised criminal gangs. Whilst there is *** linked to the Sharifizindashti network, *** it does appear that the IIS are looking to develop relationships with such groups in the UK. MI5 told the Committee that the IIS are:

> *casting around for mercenaries and operatives to conduct activity *** to build new alliances and relationships ... ***.*[146]

172. The use of a wide range of organisations means physical threat can manifest from a much broader pool of suspects, adding a further layer of unpredictability. As MI5 explained:

> *It is not typically Iranian nationals that are conducting the operations themselves. There are sometimes Iranian nationals but quite often they use other nationalities, they use criminal groups that you wouldn't at all expect to be involved in this kind of activity and they are effectively just mercenaries, they are hired for money to do the operational activity for the Iranian state. ***"*[147]

173. MI5 also told the Committee that some of the criminal groups used by Iran to conduct operational activity have links to Russia. The use of criminal groups carries both advantages for the IIS – in terms of increased deniability and the ability to conduct operations overseas where the IIS do not have a presence – and disadvantages, as there is less control over operations and variable capability.

Potential actors: militant and terrorist groups

174. Iran may also use its network of aligned militant and terrorist groups in the Middle East to prepare for hostile operations in the UK. For example, it is likely that individuals linked to Lebanese Hizbollah have been recruited in Lebanon and tasked with travelling to the UK to collect information. Lebanese Hizbollah has been involved in stockpiling explosive precursors across the world, including in the UK, in preparation for hostile operations.

175. In addition, Lebanese Hizbollah has previously met members of the New IRA, the Irish Republican terrorist group. ★★★. Following the arrest of senior New IRA members in August 2020, it appears unlikely that the remaining leadership of the New IRA will pursue links with Lebanese Hizbollah and it is probable that Iran recognises the risks of engaging with the New IRA.

[145] Oral evidence – Home Secretary, 6 July 2023.

[146] Oral evidence – MI5, *** June 2023.

[147] Oral evidence – MI5, *** June 2023.

176. As already noted, despite Iran's use of militant and terrorist groups, MI5 told the Committee that its current investigative focus is on ***, as they represent the greater national security threat to the UK.

Possible attacks: assassination

177. As noted above, Iran poses a significant assassination threat to UK-based opponents of the Iranian regime. Whilst Iran has not yet assassinated anyone in the UK, there have been multiple threats of this nature in recent months.

178. Between 2015 and 2019, Iran killed four dissidents in Europe – two in the Netherlands and two in Turkey – including one British-Iranian national. These attacks indicate that the IIS will assassinate dissidents, particularly if they feel forced to act and where they consider that the benefits of such an operation (for example preventing the sharing of sensitive information or criticism of the regime) outweigh the risks. It is probable that any Iranian decision to assassinate a dissident in the UK would be driven by factors *** (although, as previously noted, since 2022 the risk appetite of the Iranian regime to attempt assassinations of dissidents and Farsi-language journalists in the UK has increased significantly).

179. Despite the Intelligence Community's assertion that the UK is a difficult operating environment, Sir Richard Dalton claimed that: "*state terrorism is a significant threat … my own hunch … is that it is actually quite easy to kill somebody in the United Kingdom, what Iran has been doing with these … plots is throwing scares into people and showing capability and capacity to encourage people to cease activities*".[148] However, when we questioned the Intelligence Community, we were provided with a more nuanced picture. MI5 told the Committee: "***".[149]

Examples of Iranian assassination operations in Europe

The Netherlands

Mohammed Reza Kohlahi Samadi – An Iranian national based in the Netherlands living under the alias Ali Motamed was a member of the Mujahideen-e-Khalq (MEK), an Iranian opposition group. Iran alleged that he was involved in an MEK bombing in Tehran in 1981. He was murdered in 2015 in the Netherlands by two assassins paid by Naoufal Fassih, a Dutch-Moroccan citizen involved in serious organised crime. Fassih was paid EUR 130,000 for the murder by a currently unidentified source and was convicted of Samadi's murder. The IIS very probably orchestrated Samadi's assassination – if so, it would represent the first successful covert Iranian lethal operation in Europe for 25 years.

Ahmad Mola Al Nissi – An Iranian national based in the Netherlands and former president of the Arab Struggle Movement for the Liberation of Ahvaz (ASMLA), an Iranian separatist group. Iran alleged that he orchestrated attacks in Iran. He was assassinated in 2017 in the Netherlands ***.

[148] Oral evidence – Sir Richard Dalton, 23 March 2023.

[149] Oral evidence – MI5, *** June 2023.

Turkey

Saeed Karimian – A British-Iranian national based in Turkey and founder of the television channel, Gem TV, which dubs foreign films into Farsi for Iranians. He was sentenced by an Iranian court in absentia to six years in prison for circulating anti-regime propaganda (and was also allegedly linked to the MEK). He was assassinated in Istanbul in 2017 by the Sharifizindashti network. *** one of the individuals involved in the preparatory targeting work for that assassination was based in the UK.

Masoud Molavi – An Iranian national based in Turkey and former cyber security contractor for the Iranian government. He leaked sensitive information about Iranian cyber capabilities and Iranian government officials and operated a Telegram group criticising the Iranian regime. He was assassinated in Istanbul in 2019 by the Sharifizindashti network, almost certainly to stop him from sharing sensitive information.

Possible attacks: kidnap

180. Whilst Iran does have the capability to kidnap individuals from within the UK and exfiltrate them to Iran, this is a resource-intensive option and would be highly likely only to be considered where other methods have failed (as explored in more detail below, the IIS prefer to lure a target *** to a third country from where they are forcibly returned to Iran).

181. Nonetheless, the Iranian regime has been known to kidnap dissidents abroad. For example, in 2021, the US Federal Bureau of Investigation (FBI) indicted a MOIS network for plotting to kidnap a US-based journalist and human rights activist from her home in New York. The same MOIS network monitored individuals in the UK, Canada and the United Arab Emirates (UAE). As with other physical threats, it is primarily directed at Iranian dissidents: it does not appear that Iran poses a kidnap threat to mono-British nationals in the UK.

182. Dissidents of interest may be more susceptible to IIS kidnap than lure/forced repatriation operations (particularly in Iran's near abroad where the IIS are able to operate more easily). Any individual who recognises that they are of interest to the IIS will no doubt be wary of overseas travel unless they organise it themselves.

Examples of Iranian kidnap operations

Abbas Yazdi – A British national who had lived in Dubai for over ten years. Yazdi provided evidence against the National Iranian Oil Company as part of a long-running commercial legal dispute with the UAE-based company, Crescent Petroleum.

In 2013, he was abducted from Dubai and later died, reportedly during transfer to Iran. It is difficult to ascertain definitively whether MOIS or IRGC Quds Force (IRGC-QF) was responsible for the abduction although ***.

***. (The options available to HMG to protect nationals living overseas are more limited than to protect individuals living in the UK.)

***

Jamshid Sharmahd – A German-Iranian who was based in the US and a member of Tondar, an Iranian monarchist group. Iran alleged that he was involved in an attack on an Iranian mosque in 2008.

In 2020, he was kidnapped in Dubai by MOIS whilst transiting from the US to India for a business trip and forcibly repatriated to Iran. ***.

The abduction of Yazdi and Sharmahd from Dubai, a key commercial centre which attracts 1.5 million British visitors every year, and which is not geopolitically aligned with Iran, reveals Iran's capability and the potential threat to UK-based dissidents.

Possible attacks: lure and forced repatriation

183. The Intelligence Community explained that it appears the IIS's preferred methodology for forced repatriations is to lure the target *** to a third country – potentially in the Middle East which represents a more permissive operating environment *** (i.e. easier to operate in) for the IIS – from where they are forcibly returned to Iran. The JIC Chair told the Committee that Iran: "*is much more effective in its own region which it understands and where it speaks the languages*".[150] It is doubtless easier for Iran to lure someone to a country which is perceived to be less aligned to Iran or has a stronger domestic legal framework (i.e. the individual may think that they will be better protected in such a country), which may be why the IIS have previously lured dissidents to Turkey.

184. Since 2015, Iran has conducted several (***) such operations against Iranian dissidents in Europe. In 2020, MI5 assessed that ***. However, Iran is assessed still to conduct assassinations, depending on the options available to it. The Intelligence Community assessed in *** that ***, it was likely that the IIS would pursue the forced repatriation of an Iranian dissident who was based in the UK. It is very probable that Iranian forced repatriations are primarily motivated by concerns relating to the target than bilateral issues with a particular country (such as the UK).

185. The IIS use different methods to lure dissidents to travel from the UK (and other Western countries). For example, setting up fake 'personae' online to contact individuals of interest. ***. Other methods include using romantic approaches to initiate contact with targets and persuade them to travel to a third country. For example, in ***, an Iranian national resident in the UK, who worked ***, travelled to *** to meet an individual that they had met online. ***. Whilst the individual returned to the UK with the assistance of HMG, it is likely that they were lured to *** as part of an operation to attempt to force them to return to Iran.

186. Once dissidents are returned to Iran, they are often forced to 'confess' their alleged offences (such as terrorism) which are aired on Iranian state television, providing a deterrent

[150] Oral evidence – JIO, *** June 2023.

to other dissidents around the world and demonstrating the international capability of the IIS. It is likely that Iran prefers to repatriate dissidents forcibly rather than assassinate them overseas, in part due to the propaganda opportunities that derive from the judicial process.

Examples of Iranian 'lure and forced repatriation' operations in Europe

Ruhollah Zam – A France-based anti-Iranian regime journalist who ran Amad News. The Iranian regime alleged that Amad News incited protests in Iran in 2017/2018. In 2019, Zam was lured to Iraq by his Amad News colleague, believing that he would be meeting a senior Shi'a cleric (despite warnings from the French security services not to travel to Iraq). His colleague was likely an IRGC agent. He was kidnapped by the IRGC and forcibly repatriated to Iran where the Iranian media aired a confession (likely given under duress). He was sentenced to death and executed in 2020.

Habib Chaab – was based in Sweden and head of ASMLA, an Iranian opposition group. In 2020, Chaab was lured to Turkey by a MOIS agent under the pretence of marriage (despite warnings from the Swedish authorities not to travel to Turkey). He was kidnapped by the Sharifizindashti criminal network and forcibly repatriated to Iran where the Iranian media aired a confession (likely given under duress) that he had been working for Saudi Arabia. Iran alleged that he was responsible for an attack on a military parade within Iran in 2018 and he was executed in 2023.

Both Zam and Chaab were also previously targeted ***.

Possible attacks: terrorist attacks

187. As noted previously, beyond the targeting of dissidents, organisations critical of the regime, and Israeli and Jewish interests, the Intelligence Community judge that there is only a remote chance that Iran will conduct a physical attack in the UK against a member of the general public. Nevertheless, Iran has conducted terrorist activity around the world – particularly through IRGC-QF – in order to further its national security and foreign policy objectives. This includes using terrorist attacks to degrade its primary political and diplomatic enemies, including Israel and MEK. As noted earlier in the Report, previous examples include an attempt by MOIS to use an explosive device to target an MEK conference in Paris in 2018, which was disrupted by European intelligence services.

188. Iran and its allies have also been linked to preparations for terrorist attacks, including reconnaissance of targets and stockpiling of explosive precursors in case the Iranian regime determines that such an attack is required. One example is the IIS gathering intelligence on Israeli/Jewish targets ***. The JIC Chair recalled another example: a shooting at a German synagogue in 2022, which he said had "*the Iranian hand behind it*".[151]

[151] Oral evidence – JIO, *** June 2023.

Operation CARAWAY:[152] *disruption of Lebanese Hizbollah attack planning*

In September 2015, MI5 and law enforcement disrupted Lebanese Hizbollah activity in the UK. Over 20,000 first aid kits were seized from five properties in London, one of which was linked to a member of Lebanese Hizbollah. Each first aid kit included an ice pack which contained the explosive precursor, ammonium nitrate, which if extracted could have produced approximately 3.5 tonnes of explosive material. Fewer than ten packs were needed to produce a small explosive device.

MI5 assessed that Lebanese Hizbollah was stockpiling as part of its contingency planning should Iran or Lebanese Hizbollah judge that an attack was necessary. This activity was replicated across Europe, North America and parts of Asia. ***

189. Given that we heard throughout this Inquiry that Iran does not view attacks on dissident, Israeli or Jewish targets in the UK as attacks on the UK, we questioned whether that made the chance of an attack relatively likely. MI5 told us:

> *we have seen longstanding intent against Jewish/Israeli targets in the UK, particularly where those individuals or targets are seen as undermining the Iranian regime ... it is seen through the lens of either internal security of the regime or ... retaliation for a specific grievance ...* [however,] *the majority of the threat we have seen recently has been focussed at media organisations, rather than Jewish/Israeli targets, and we haven't seen an increase in the threat to Jewish/Israeli targets in the last few months.*[153]

How will the physical threat evolve?

190. The Intelligence Community predict that Iran is likely to remain a key state kidnap threat to the UK for the foreseeable future (***). The IIS will almost certainly continue to consider lure/forced repatriation operations in the future as an option to target dissidents overseas.

191. It appears that the recent increase in the physical threat posed by the IIS to UK-based individuals indicates that Iran's intent has increased – and the threat could continue to increase rapidly if Iran's intent or capability develops further (***). As the Home Secretary explained:

> [it will] *turn on events in the region, events internally in Iran. If we look at how the IRGC operates, it is all about survival and protection and quite a jealous and ...* [an] *active defensive approach, defending the reputation of the Iranian*

[152] In some instances in this Report, we have substituted an ISC-specific code word where it has been necessary to refer to the name of an operation or project, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to real operation names. The ISC code words have no operational significance.

[153] Oral evidence – MI5, *** June 2023.

> *regime, defending the authority of the Supreme Leader, snubbing out and, you know, to put it crudely, killing off any dissidents and voices who are challenging or calling into question the methods, the policies, and the practices by the regime ... when we saw the protests ... in the autumn, that really was a bit of a turning point in terms of the activity that we saw by the regime here in the UK and against UK-based individuals.*[154]

After the killing of Soleimani

192. The Intelligence Community said that they are continuously monitoring for any intelligence (***) to indicate that Iran or its network of affiliated militant organisations in the Middle East were planning to conduct a terrorist attack in the UK as retaliation for the 2020 US killing of IRGC-QF Commander Qasem Soleimani (although, as noted above, ***). It is possible that the killing will inspire lone actors to launch attacks that are not directed by Iran or its network of aligned militant organisations.

V. There has been a significant increase over the last 18 months in the physical threat posed by Iran to those residing in the UK. There have been at least 15 attempts at murder or kidnap against British nationals or UK-based individuals since the beginning of 2022. The threat of physical attack on individuals in the UK is currently the greatest threat we face from Iran and is now on a broadly comparable level with Russia.

W. The Iranian physical threat in the UK is focused acutely on dissidents and other opponents of the regime. The targeting of dissidents is one of the Iranian Intelligence Services' highest priorities, and Iran is prepared to assassinate dissidents in the UK.

X. Iran does not view attacks on dissident, Jewish and Israeli targets in the UK as attacks on the UK. It rather sees the UK as collateral in its handling of internal matters – i.e. removing perceived enemies of the regime – on UK soil.

Y. The Iranian Intelligence Services have shown that they are willing and able – often through third-party agents – to attempt assassination within the UK, and kidnap from the UK, although in respect of the latter they prefer to lure individuals * to a third country in which the Iranian Intelligence Services can operate more easily, and forcibly repatriate them from there.**

Z. The Iranian Intelligence Services are increasingly using organised criminal gangs to undertake hostile activity abroad. Some of the criminal groups used by Iran to conduct operational activity have links to Russia. The use of such gangs provides deniability for Iran. In addition, the wide range of organisations used means a broad pool of suspects – adding a further layer of unpredictability.

[154] Oral evidence – Home Secretary, 6 July 2023.

THE THREAT: NUCLEAR PROGRAMME

193. In 2021, the UK Government published its Integrated Review,[155] which recognised that countering proliferation around the world, including in the Middle East, was critical for the UK's security and prosperity, for maintaining regional and global security, reducing threats to UK citizens and the Armed Forces, and facilitating safe trade for UK industry.

194. The most likely cause of further nuclear proliferation is Iran proceeding with its nuclear weapon programme. As the Chief of SIS told the Committee: "*if any country gets nuclear weapons ... it sets off a chain reaction in the region and it must make other countries in the region consider whether they might need to invest in the same technology*".[156] Clearly Iran proceeding to develop a nuclear weapon would pose a threat to UK nationals in the region and possibly a direct physical threat to the UK mainland. It could also lead to regional nuclear proliferation, forcing Saudi Arabia – a key Iranian adversary – to obtain nuclear weapons, and exacerbate broader regional instability. The Committee therefore agree with Sir Richard Dalton's statement that: "*the proliferation issue is a serious threat to the security interests of the United Kingdom*".[157]

Iran's previous attempts to develop a nuclear weapon

195. From the 1980s, Iran reportedly attempted to develop a nuclear weapon programme covertly and built nuclear facilities capable of providing fissile material (one of the key processes in developing a nuclear weapon). This was disrupted in 2003, when part of the programme was exposed, including through reporting from the International Atomic Energy Agency (IAEA). This contributed to the later implementation of sanctions on Iran[158] and over a decade of negotiations relating to Iran's nuclear programme, resulting in the 2015 Joint Comprehensive Plan of Action (JCPOA) nuclear agreement between Iran, the US, Russia, China, the UK, Germany and France.

2015 JCPOA nuclear agreement

196. The JCPOA provided partial sanctions relief for Iran in return for verifiable restrictions on its nuclear programme. Iran committed to only pursue civilian nuclear work and the IAEA – the UN's nuclear monitoring body – was given access to Iranian facilities to monitor compliance with the restrictions. (We consider the impact of the JCPOA later in the chapter.)

[155] The Integrated Review is covered in the 'Strategy and Policy Response' chapter later in the Report.

[156] Oral evidence – SIS, *** June 2023.

[157] Oral evidence – Sir Richard Dalton, 9 March 2023.

[158] Following the partial exposure in 2003, Iran entered into an agreement with the E3 (the UK, France and Germany) to suspend some sensitive nuclear activity, pending further negotiations. Iran subsequently reversed this suspension, beginning uranium conversion in 2005 and uranium enrichment in 2006. Iran also failed to co-operate adequately with IAEA efforts to establish the details of its previous undeclared nuclear activities. This led to the imposition of sanctions on Iran.

2018 US withdrawal from the JCPOA

197. In 2018, the then US President Trump announced that the US was leaving the JCPOA and reimposing those US sanctions lifted under the deal. This was on the stated grounds that Iran's destabilising regional activity, including its development of ballistic missiles, was not addressed in the JCPOA. The Trump administration advocated a new, broader agreement that included restrictions on Iranian ballistic missiles and the cessation of Iranian support for proxy groups.

198. The US's withdrawal left the JCPOA – in the words of the then UK Foreign Secretary – as a "*shell of an agreement*".[159] The US withdrawal was criticised by the remaining signatories to the deal; the UK, France and Germany issued a joint statement that they regretted the US decision, and the EU said that it was determined to preserve the deal. Russia and China also condemned the US decision to withdraw.

199. Subsequently, in 2019, Iran announced that it would renege on its JCPOA commitments and engage in prohibited nuclear activities. Iran threatened to increase its non-compliance every 60 days, unless the remaining signatories could provide sufficient economic relief within 30 days. Whilst the three European signatories to the JCPOA – the UK, France and Germany – devised a response to facilitate Iranian trade, Iran deemed it insufficient as a response to the effects of US sanctions on its economy.

Iranian nuclear intent and objectives

Intent

200. Our External Experts had different views as to whether Iran had the intent to develop a nuclear weapon. Baroness Ashton highlighted the plurality of opinion within the Iranian regime:

> *There were definitely different views within the* [Iranian] *government ... a complete spectrum of opinion, from those who are very hard-line on saying "We have to have a nuclear weapon, whatever the cost" to those who thought that, actually, it was not in Iran's interests to have a nuclear weapon, and one of the challenges with Iran is that that difference of opinion still exists.*[160]

201. Dr Vakil suggested that the Iranian regime was intentionally pursuing a strategy of '*nuclear ambiguity*'. This aimed to:

> *leverage its nuclear programme when opportunistically possible in order to ... protect its security and stability ...* [and] *should Iran militarise its programme ... Iran would lose significantly its posture in the Middle East, it would lose the benefit of being a threshold state that is on the precipice ... should it weaponise, it would invite perhaps military attack ... it would also see a cascade of perhaps*

[159] 'Comments in Parliament on "Iran"', *Hansard*, 13 January 2020.

[160] Oral evidence – Baroness Ashton, 21 March 2023.

> *other regional states advance their own programmes. So, the advantage that it currently has in maintaining nuclear ambiguity would be completely lost.*[161]

202. Ambassador Bolton disagreed, emphasising that the regime has had a longstanding desire to obtain a nuclear weapon, stating:

> *I don't think we have detected, over the last 25 years, any change in the determination of the regime, the regime as a whole, to get a nuclear weapons capability ... the evidence is actually pretty clear that they are working towards that goal ... I don't think there is any ambiguity about the Iranian strategic decision to get nuclear weapons. I think they have engaged in activity that is simply inconsistent with any behaviour other than weaponisation.*[162]

203. It seems that the Iranian Supreme Leader, Ayatollah Khamenei, wants to maintain the option of developing nuclear weapons. Nonetheless, the US Intelligence Community have previously publicly stated that it appears very unlikely that he will have taken the decision to restart a concerted programme to develop and produce a nuclear weapon: in 2021, the US Central Intelligence Agency (CIA) Director Bill Burns publicly stated that his agency "*doesn't see any evidence that Iran's Supreme Leader has made a decision to move to weaponise*";[163] and in 2022, the Annual Threat Assessment published by the Office of the US Director of National Intelligence stated that "*Iran is not currently undertaking the key nuclear-weapons development activities that we judge would be necessary to produce a nuclear device*."[164]

204. The Chief of SIS told the Aspen Security Forum in 2022 that "*I don't think the Supreme Leader of Iran wants to cut a deal, but the Iranians won't want to end the talks either*".[165] In evidence to this Inquiry, the JIC Chair told the Committee: ***.[166] The Chief of SIS agreed: ***.[167]

205. As Sir Richard Dalton explained, this provides Iran with a "*threshold capability*". He noted that "*they want to be like Japan, they want to be like Brazil, Sweden, countries who have the technical know-how and could move to weaponisation if they felt so threatened*".[168]

206. Whilst HMG acknowledged that it is difficult to predict the precise circumstances in which Iran would proceed to develop a weapon, its long-term estimation in 2021 was that ***. It also judged that there was a realistic possibility that Iran could develop ***.

[161] Oral evidence – Dr Sanam Vakil, 21 March 2023.
[162] Oral evidence – Ambassador John Bolton, 21 March 2023.
[163] 'CIA Director on Today's Global Challenges', Wall Street CEO Council, 6 December 2021.
[164] '2022 Annual Threat Assessment of the U.S. Intelligence Community', Office of the US Director of National Intelligence, 8 March 2022.
[165] Chief of SIS comments at the Aspen Security Forum, 21 July 2022.
[166] Oral evidence – JIO, *** June 2023.
[167] Oral evidence – SIS, *** June 2023.
[168] Oral evidence – Sir Richard Dalton, 9 March 2023.

207. The Iranian regime will clearly be conscious of the risk that the creation of a nuclear weapon will make Iran an even greater pariah on the international stage. The JIC Chair explained:

> *Iran also likely knows that, if it developed and had a nuclear weapon, it would lose massive amounts of support, it would find it extremely difficult *** this was justified and, therefore, having a nuclear weapon carries risk for them as well as potential advantage.*[169]

208. Iran will no doubt be aware that developing a nuclear weapon could lead to a US and/or Israeli military intervention. As the JIC Chair noted, the Iranian regime would be "*much more worried about* ***"[170] – although he noted that the effectiveness of any military action would be a factor.

209. One further consideration in understanding Iranian intent is the Supreme Leader's potential fatwa[171] against nuclear weapons. Whilst its existence and significance is debatable,[172] the JIC Chair told us: "*this is not an insignificant factor …* [it says more about] *the Supreme Leader's approach and mentality to nuclear weapons than it does* [about] *creating a formal barrier against it*".[173]

Objectives

210. Regardless of whether a fatwa against nuclear weapons exists or not, the Iranian Supreme Leader may nevertheless wish to maintain the option of developing nuclear weapons as the ultimate security guarantee: as has already been described, the safety and security of the Iranian regime is Iran's primary objective. Dr Vakil noted: "[Iran's] *nuclear programme alongside asymmetrical defence has been its strategy to protect its security and stability*".[174]

211. Our External Experts also suggested – to different extents – that Iran's desire to maintain the option for developing a nuclear weapon may also be due to its objective to be a leading regional power. For example, Baroness Ashton told the Committee that: "*the point about nuclear weapons for them* […] *is their dominant role in the region*".[175] Ambassador Bolton agreed, stating that Iran:

> *seeks nuclear weapons to dominate others, not for defensive purposes, to achieve hegemony in the region … I think they saw the route towards being a nuclear power as a high card in any developments in the region, so that it was*

[169] Oral evidence – JIO, *** June 2023.

[170] Oral evidence – JIO, *** June 2023.

[171] A fatwa is a ruling on a point of Islamic law given by a recognised authority.

[172] It is not clear whether the fatwa exists or if it is binding. As Abbas Milani, the Director of Iranian Studies at Stanford University, states: "*The issue of the fatwa is complicated. Whether it actually exists and even whether Mr. Khamenei* [the Supreme Leader] *is entitled to issue fatwas and finally how changeable are fatwas are all contested matters*." – 'Did Iran's Supreme Leader issue a fatwa against the development of nuclear weapons?', *The Washington Post*, 27 November 2013.

[173] Oral evidence – JIO, *** June 2023.

[174] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[175] Oral evidence – Baroness Ashton, 21 March 2023.

> *an objective that would put Iran … beyond contest once it developed the ability to use nuclear weapons, really at its discretion.*[176]

212. Dr Vakil took a different view, considering that Iran's nuclear programme is not about the region. She said:

> *Iran has regional strategic depth. Iran has demonstrated that it has developed significant indigenous defence capabilities far beyond regional states. So it has its own ability to advance security in the region, compared to Saudi Arabia and the Gulf states, except for Israel. So its nuclear programme is about protecting itself from Western states … the mindset is that it constantly fears the West is seeking to overthrow Iran.*[177]

213. Baroness Ashton agreed that the Iranian regime is motivated by its fear of foreign intervention, particularly in terms of regime change, and that the Iranian regime thinks:

> [regime change] *was the objective of much of what the UK, the US, or the West, would be doing and therefore I think they saw nuclear weapons as one of the ways to prevent that … in a region where they felt they wanted to be dominant and where they sensed there was a lot of hostility.*[178]

214. When we questioned the Intelligence Community on Iran's objectives, they acknowledged the potential link between the option to develop a nuclear weapon and Iran's overarching goal to maintain the security of the regime. Iran may well want a capability to construct a nuclear weapon *** should the regime feel that its survival is under threat from external forces.

215. It can also be seen that Iran uses its nuclear programme as leverage to apply pressure on the international community as part of negotiations relating to its nuclear programme or other unrelated issues, such as the application of sanctions. For example, if the nuclear negotiations are not proceeding as planned, Iran may announce a progression in its nuclear programme to put pressure on the other parties to negotiate further.

Iranian nuclear decision-makers and actors

216. The Committee was told that "*ultimately,* [the Supreme Leader] *will decide whether or not they go forward with a* [nuclear weapon] *programme*".[179] Nevertheless, the President may have some influence over nuclear policy and international negotiations on a revised nuclear deal, including aspects relating to sanctions, given his responsibility for economic affairs. Media reporting suggests that the political leanings of successive Iranian Presidents can sometimes have an influence on Iranian nuclear policy: for example, former President

[176] Oral evidence – Ambassador John Bolton, 21 March 2023.

[177] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[178] Oral evidence – Baroness Ashton, 21 March 2023.

[179] Oral evidence – ***, *** June 2023.

Hassan Rouhani (in office 2013–2021) was considered to be a more moderate voice on nuclear negotiations than President Ebrahim Raisi.[180] Dr Vakil explained how the differing approaches of Iranian Presidents can shift the direction of Iran's nuclear policy:

> *Depending on who is in power, the regime can produce more of a debate inside the country or less of a debate ... The regime is united in self-preservation, stability and security; they are very divided on how to employ the tools they have in order to achieve* [these goals] ... *reformers like President Khatami or pragmatists like President Rouhani saw the nuclear programme as an opportunity to advance their economic interests ... this was seen as a leverage-building exercise ... whereas conservatives and hardliners see the nuclear programme more in this security-minded worldview ... today there is a monopoly of conservative power in Iran and the reformists and pragmatists are clearly not very influential in the state.*[181]

217. When we questioned how the Iranian nuclear threat would be affected by the election of President Raisi, the Intelligence Community noted that it was well known that he was more hard-line and it was widely assumed that he would adopt a tougher stance than his predecessor in relation to negotiating a revised nuclear deal with the international community. However, it appears to be unlikely that President Raisi would change Iran's overarching direction – given that the Supreme Leader is the ultimate decision-maker in consultation with the Supreme National Security Council (SNSC). *** noted that: "***".[182]

218. In terms of the involvement of the Iranian Intelligence Services (IIS) in the development of a nuclear weapon, Ambassador Bolton told the Committee that the Islamic Revolutionary Guard Corps (IRGC) has used the Atomic Energy Organisation of Iran as a 'front' for work relating to nuclear weapon development. He said that the nuclear programme is "*driven by the IRGC …* [but] *it is not only the IRGC. There is a whole establishment in Iran … that brings together the IRGC, alongside security intelligence forces, as well as economic entities, and together they see this as an investment*".[183] The Intelligence Community provided the Committee with a broadly similar view: "*if a decision was taken to pursue* [a nuclear weapon], *** *that is probably the sort of chain of command that you would be seeing*".[184]

Iranian nuclear capability

219. In order to develop a nuclear weapon, Iran would need to obtain a sufficient amount of fissile material (for example weapons-grade highly enriched uranium or plutonium) and to complete a 'weaponisation' process. The two key determinants of Iranian nuclear weapon capability therefore are the 'Breakout Time' and 'Weaponisation Time'.

220. The Breakout Time refers to the minimum plausible time it would take Iran to produce the necessary fissile material for a first nuclear device and the Weaponisation Time refers to

[180] Although this does not necessarily follow: for example, DI told us that the peak of Iran's previous nuclear weapons work took place during the reformist administration of President Mohammad Khatami, ***.

[181] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[182] Oral evidence – ***, *** June 2023.

[183] Oral evidence – Ambassador John Bolton, 21 March 2023.

[184] Oral evidence – JIO, *** June 2023.

the time needed to develop, manufacture and prepare a deliverable weapon. Given that Iran has reduced its Breakout Time, the Weaponisation Time is increasingly the most important factor in determining how quickly Iran could develop a nuclear weapon.

Breakout Time and Weaponisation Time

221. In 2019, the JIC judged that it would take Iran at least *** to build a deliverable nuclear weapon. However, this time has reduced in recent years.

222. The JIC Chair told the Committee that this had reduced further following the US withdrawal from the JCPOA. In mid-2019, when Iran remained within JCPOA limits on uranium enrichment, DI assessed that Breakout Time was over a year (***). However, by mid-2021, DI assessed, drawing on IAEA reporting, that this had reduced to a few months (***). As of mid-2023 – with Iran having accumulated a far larger stockpile of enriched uranium, including 60% high enriched uranium – DI assessed that Iran could further enrich enough to 90% (known as 'weapons grade') for a first device in a very short time, perhaps as little as weeks (***).

223. With regard to the Weaponisation Time, the Intelligence Community assessed that the potential timelines have also reduced over the last few years. They now assess that Iran is probably capable of producing a testable device in ***, and a deliverable nuclear weapon in ***. However, there is a realistic possibility that Iran could produce a nuclear weapon in an even shorter timeline – i.e. a testable version between *** and a deliverable weapon within ***. It is worth noting that *** fissile material production, ***.

224. The Intelligence Community *** their assessment of the Iranian Breakout Time; however, we note that *** regarding the assessment of potential weapon development (i.e. Weaponisation Time). The UK – and perhaps the rest of the international community – may therefore have *** notice period before Iran is able to conduct a nuclear weapons test. We explore this *** in more detail later in the Response section of this Report.

Iranian nuclear international partnerships

225. The Committee asked the Intelligence Community whether Russia and China would help Iran with its nuclear programme, particularly given the recent increase in co-operation. The JIC Chair told us: "*it is not in the interests of either Russia or China that Iran achieves a nuclear weapon … I don't think … *** I expect to see Russia or China helping Iran to acquire a nuclear weapons capability*".[185] Baroness Ashton had expressed the same view, telling the Committee: "*the animosity of Russia towards the idea of an Iranian nuclear programme was pretty clear to see. My discussions with President Putin made that very clear*".[186] However, ***. We also questioned whether Russia and China might collaborate with Iran in terms of insights into the negotiating stance of the West around Iran's nuclear programme.

226. Ambassador Bolton also emphasised the potential increase in the nuclear threat posed by the relationship between Iran and North Korea. As previously noted, he stated:

[185] Oral evidence – JIO, *** June 2023.

[186] Oral evidence – Baroness Ashton, 21 March 2023.

> *This connection between North Korea and Iran, which we do not fully know about or understand, is something that should be in our minds at all times, because we know that the North Koreans have detonated six nuclear devices and that they are working rapidly to develop warheads that they can place on top of ICBMs* [intercontinental ballistic missiles] *and if that information is being shared with Iran – and we just don't know one way or the other – that is a very significant fact ... if you are a desperately poor country with nuclear weapons technology dealing with an oil-rich country that wants nuclear weapons technology, the transaction is not hard to imagine.*[187]

227. It is possible that North Korea would be willing to sell weapons-grade nuclear material to another state under some circumstances; ***. Given that North Korea is a pariah state, it is thought that Iran would be wary about collaborating with it on nuclear weapon technology as it could set Iran further apart from the rest of the international community. The JIC Chair told the Committee:

> *Because North Korea is a rogue nuclear weapons state, it is tempting to assume that* ***.[188]

However, logically, there may be closer co-operation if Iran perceived that it faced a significant external or existential threat. Such co-operation may also be more likely in a less sensitive nuclear area ***.

The 2015 JCPOA: impact on the threat

228. The Intelligence Community assess that most of the covert work on Iran's previous nuclear weapon programme was stopped when part of it was exposed in 2003. A public US intelligence assessment from 2007 stated that "*we judge with high confidence that in fall 2003, Tehran halted its nuclear weapons program ...* [i.e.] *Iran's nuclear weapon design and weaponization work and covert uranium conversion-related and uranium enrichment-related work*". The same assessment also stated that "*we judge with high confidence that the halt lasted at least several years ...* [and] *with moderate confidence Tehran had not restarted its nuclear weapons program as of mid-2007*".[189] ***.[190]

229. Ahead of the JCPOA negotiations, US intelligence officials reportedly estimated that, in the absence of an agreement, Iran could "*produce enough nuclear material for a weapon in a few months*".[191] The JCPOA aimed to restrict Iran's nuclear programme so that, if it decided to develop a nuclear weapon, the Breakout Time would be "*at least a year*" – thereby providing the international community with time to respond.[192]

[187] Oral evidence – Ambassador John Bolton, 21 March 2023.

[188] Oral evidence – JIO, *** June 2023.

[189] *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007.

[190] ***.

[191] 'What is the Iran Nuclear Deal?', Council on Foreign Relations, 21 June 2023.

[192] 'Iran's Nuclear Breakout Timeline: A Fact Sheet', Washington Institute for Near East Policy, 28 March 2015.

230. Most of our External Experts spoke of the effectiveness of the JCPOA in reducing the nuclear threat posed by Iran. Baroness Ashton and Dr Vakil viewed the JCPOA as a very positive development, helping to improve relations significantly between Iran and the West and increase international oversight over Iran's nuclear programme. Baroness Ashton – who played a significant role in nuclear negotiations with Iran on behalf of the EU – explained that:

> *it was the first agreement. It got rid of the immediate crisis of the fear of them building a nuclear weapon and it dealt with that so that we could move on to the region, to human rights, to all of the other issues, that we with great validity, wanted to talk to Iran and that we could revisit this agreement as time went on to see its effectiveness.*[193]

Dr Vakil agreed, emphasising that: "*Iran was repeatedly in compliance, reversed its nuclear programme and was, under IAEA authority, regularly inspected over the period of the deal. The international community benefited from a successful multilateral negotiation.*"[194]

231. Ambassador Bolton, however, disagreed with this assessment of the JCPOA, arguing that it was critically flawed. He told the Committee that: "*the fact that Iran has that enrichment capability* [within the JCPOA]*, that is the fundamental flaw ... as the work necessary to enrich uranium from its stated nature, 0.7% U 235, to reactor grade 3 to 5%, constitutes 70% of the work necessary to enrich to 90% weapons grade*".[195]

232. Ambassador Bolton also criticised the lack of a meaningful arms control negotiation and the inability of the IAEA to monitor all of Iran's historical nuclear weapon facilities, due to the IAEA having to rely on being permitted access. He stated:

> *the Iranians frustrated any effort to look at prior efforts to build nuclear weapons ... so it is just simply wrong to say that there was no non-compliance with the deal. The IAEA can only monitor what it can monitor and, when it is denied access to facilities, it cannot opine on what is going on there any more than anyone else, and the Iranians knew that and that is why they didn't grant them access.*[196]

233. The Intelligence Community took a similar view to Dr Vakil, noting the IAEA's reporting that Iran was observing the key JCPOA provisions regarding its uranium enrichment programme – even if, as we have noted previously, Iran may well not have abandoned its long-term aspirations for nuclear weapons. As the JIC Chair noted, the agreement was being monitored by the IAEA with an unprecedented degree of intrusion – *** – and there were not any significant examples of Iran breaching its primary obligations.

234. However, following the US's withdrawal from the JCPOA in 2018 and the reimposition of sanctions on Iran, it stopped complying with the JCPOA – this non-compliance included

[193] Oral evidence – Baroness Ashton, 21 March 2023.

[194] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[195] Oral evidence – Ambassador John Bolton, 21 March 2023.

[196] Oral evidence – Ambassador John Bolton, 21 March 2023.

plans to expand its enrichment activity. Baroness Ashton and Dr Vakil both told the Committee that in their opinion the nuclear threat posed by Iran had increased since the US had withdrawn from the deal. Baroness Ashton suggested that:

> *we now have a situation where the Iranians are very close to being able to do precisely what the JCPOA prevented them from doing ... we are now starting from a position where Iran is much much much more dangerous than it was when we had the JCPOA.*[197]

235. Dr Vakil noted that the US withdrawal had also led to an acceleration in regional instability:

> *Not only has there been an acceleration of Iran's nuclear programme, there has been an obvious turn ...* [with] *Iran using what it called maximum resistance as a strategy to push back against maximum pressure,*[198] *that saw Iran accelerate its nuclear programme, that saw Iran accelerate support for regional groups in Lebanon, Syria, Iraq and Yemen, it sought increases in transfer of lethal aid and using that lethal aid against its neighbours in Iraq, against Saudi Arabia ... we saw an uptick in Houthi attacks all through 2019 to 2022, even attacking Abu Dhabi in January of last year* [2022].[199]

236. The Intelligence Community considered that, whilst the JCPOA had had some lasting effect, ***: "*there are still elements of it that are significant, not least some of the sunset clauses have not yet timed out, ***".*[200] ***. For example, the JIC Chair told the Committee that "*over the last several months, there* [has] *been …* [one][201] *occasion on which Iranian enrichment spiked to just over 80%*". Whilst it was not clear to the IAEA why or how it happened, it was nevertheless able to identify the change. The JIC Chair explained that the "*IAEA continues to act as a tripwire, which is important and gives us some insight and assurance around what Iran is doing. ***".*[202]

How will the Iranian nuclear threat evolve?

237. Our External Experts all considered that it was very difficult to predict how the nuclear threat was likely to change in the future, given the different variables involved. Dr Vakil noted this complexity:

> *I think that nuclear investment alongside all of the other asymmetric tools will continue to develop but the nuclear, I think, is the most risky for Iran ... It remains to be seen how the nuclear issue evolves: it could develop into something more*

[197] Oral evidence – Baroness Ashton, 21 March 2023.

[198] The US policy of 'maximum pressure' refers to the policy started under the administration of President Trump to leave the 2015 JCPOA nuclear deal and reimpose sanctions on Iran.

[199] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[200] Oral evidence – ***, *** June 2023.

[201] In the evidence session in June 2023, the JIC Chair originally told the Committee that there had been two occasions in 2023 where enrichment was detected above 80%. The JIO subsequently corrected this evidence, confirming that there had been only one occasion.

[202] Oral evidence – JIO, *** June 2023.

> *escalatory, but it also could not. There are many pieces of this chessboard that are moving simultaneously, from Israeli–Iran grey zone tensions, from Iran–Saudi dynamics, but also a broader possibility of defining a new deal – a bigger, better deal or a smaller, shorter deal. There are so many different variables and options and scenarios on the table.*[203]

238. Some of the potential future developments might be the negotiation of a limited successor to the JCPOA or a new wider security framework but there is also the possibility of military strikes against Iranian nuclear infrastructure. These options are explored below.

(i) A possible new JCPOA agreement

239. Following the lack of progress in negotiating a successor to the JCPOA agreement since 2018, sanctions remain imposed on Iran, and Iran has taken further steps in terms of non-compliance, which it is highly likely are intended to build leverage in any future negotiations and to develop capabilities that would support weapon development. It is possible that Iran wants to achieve at least some sanctions relief via a renegotiated nuclear deal: indeed, some of Iran's destabilising regional activity since 2018 may have been aimed at achieving that. In the event that negotiations fail or the deal collapses entirely, that surely will lead Iran to continue further to expand its nuclear programme.

240. The Foreign Secretary told the Committee that he regularly discussed the future of the JCPOA and alternative arrangements with international partners, ***

> *deadlines are looming but we are working with the *** and the *** on what happens next ... it is ongoing work and I don't have something in my back pocket to say "oh well, at the point where, you know, the JCPOA basically gets timed out, we would replace it with this"; but we are speaking regularly and intensely with our partners on this issue.*[204]

The 'deadlines' that the Foreign Secretary refers to are the restrictions imposed on the Iranian nuclear programme as part of the JCPOA (such as the testing and production of certain centrifuges[205]) that will expire over the next few years. The Committee is concerned that the Foreign Secretary was unable to articulate what alternative arrangements might look like or to point to a workable solution, with deadlines approaching.

(ii) A possible new regional security framework

241. Most of our External Experts saw value in pursuing a longer-term security framework in the region (that dealt with Iran's ballistic missile threat and its support to militant and terrorist groups, for example) but noted the significant difficulties involved. For example, Sir Richard Dalton criticised that the UK has "*never tried to establish credibility for the idea of long-term security arrangements in this volatile part of the world ... we have never*

[203] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[204] Oral evidence – Foreign Secretary, 6 July 2023.

[205] A device used at nuclear facilities to enrich uranium so that it can be used to produce power (in either a nuclear reactor or a nuclear weapon).

encouraged diplomacy across lines of enmity in the Gulf to try and decrease layers of tension".[206] As noted above, Baroness Ashton said that one of the benefits of successfully negotiating the JCPOA agreement was that the political momentum could have been used to address other issues such as regional security. She said: "*My big regret is that we stopped and we should have carried on ... to the next agreement and the next ... my big fear is we have lost it all.*"[207] Ambassador Bolton disagreed: in his view, one of the flaws of the original JCPOA was its failure to cover regional security (although he also noted that he would not have believed any commitment from Iran to stop supporting terrorism).[208]

242. The Deputy National Security Adviser (DNSA) was *** about whether such a regional security framework was currently realistic. In his view, the only immediately apparent alternative was an improvement in the relationships between Iran and other states, such as ***. He considered that:

> *something bigger, broader, structural – it seems so kind of fanciful that I am not sure that there is anything that immediately comes to mind that would take us into a much better place.*[209]

243. The Chief of SIS broadly agreed, stating that whilst "*it is still clearly government policy to find some way towards a negotiated prevention of Iran acquiring a nuclear weapon, whether that is a restoration of JCPOA or something else, *** there is no kind of overarching architecture I can see looming out of the mist, I really can't*".[210] He noted other agreements in place, such as that brokered by China between Saudi Arabia and Iran.

244. If Iran were to agree a wider regional security framework (for example, including constraints on its missile capability), Iran would presumably demand substantive security concessions in return (for example, reduced Western military presence or reduced Western arms exports to Iran's regional adversaries). Iran's willingness to negotiate would also probably depend on its perception of threat and opportunity in the region – for example, the level of US armed forces, Israeli attacks, and possible regional instability.

245. *** Iran would be unlikely to agree to surrender capability which it sees as central to its safety and security. ***.[211]

(iii) A potential military attack on Iran

246. The Intelligence Community judged in 2021 that a durable deal on Iran's nuclear programme and/or significant progress in bilateral talks between Iran and Saudi Arabia and the UAE would reduce wider regional tensions. Conversely, failure to secure an agreement on Iran's nuclear programme "***".[212]

[206] Oral evidence – Sir Richard Dalton, 9 March 2023.
[207] Oral evidence – Baroness Ashton, 21 March 2023.
[208] Oral evidence – Ambassador John Bolton, 21 March 2023.
[209] Oral evidence – DNSA, *** June 2023.
[210] Oral evidence – SIS, *** June 2023.
[211] Written evidence – JIO, 24 August 2021.
[212] Written evidence – JIO, 9 August 2021.

247. It is possible that one or more of Iran's regional adversaries will attack Iran's nuclear facilities in the future. ***. If Iran's nuclear facilities were attacked, ***.

248. The Intelligence Community noted that the threat to the UK from Iran would increase dramatically if the nuclear situation changed significantly in the region and military action were taken against Iran. The Chief of SIS told the Committee:

> ****. If it does, the threat levels across all these various dimensions … all shoots up.*[213]

Military action taken against Iran must surely increase the threat to a range of UK interests – for example, military bases, energy interests in the region, dual-nationals and British Embassies in the region. Iranian risk appetite for covert hostile activity in the UK would probably also increase. The extent of these potential threats would presumably depend on the extent to which Iran perceives the UK to have been involved in any military action.

Could a nuclear Iran lead to an increased terrorist threat?

249. Ambassador Bolton warned that, from a UK security perspective, the biggest threat from a nuclear-armed Iran "*comes from the possibility that the government of Iran would sell or give nuclear technology, a nuclear device, to a terrorist group*".[214] When the Committee put this to the Intelligence Community, *** it views Iran as a rational actor which cares about its international position. The JIC Chair noted: "***".[215]

AA. Nuclear proliferation around the world, including in the Middle East, is a critical threat to the UK on a number of levels. Iran proceeding with its nuclear weapons programme therefore poses a threat both to UK nationals in the region and to the UK mainland – and to global security more broadly if it led to regional nuclear proliferation and exacerbated regional instability.

BB. It appears that Iran has not yet developed a nuclear weapon nor taken a decision to produce one, but it maintains the option of developing one – largely as the 'ultimate security guarantee'. It is difficult to determine what would trigger such a decision by the Supreme Leader: it is plausible that Iran's intent is to maintain a state of 'nuclear ambiguity' at the threshold of weaponisation; however, it may choose to weaponise if it feels it is facing an existential threat.

CC. Whilst the 2015 Joint Comprehensive Plan of Action nuclear agreement had its limitations, the Intelligence Community believe that – before the US's withdrawal in 2018 – Iran was broadly compliant with the restrictions on its nuclear programme; this appears to have reduced the Iranian nuclear threat, if only in the short term.

[213] Oral evidence – SIS, *** June 2023.
[214] Oral evidence – Ambassador John Bolton, 21 March 2023.
[215] Oral evidence – JIO, *** June 2023.

DD. Since the US's withdrawal from the Joint Comprehensive Plan of Action, the Iranian nuclear threat has increased as Iran has taken steps in developing its nuclear programme. While it appears that it is still short of the 'weaponisation' phase, the potential timelines have reduced over the last few years and Iran has the capability to arm in a relatively short period – possibly * to produce a testable device and *** to develop a deliverable nuclear weapon.**

EE. Given the increase in the Iranian nuclear threat, negotiating a form of de-escalation between Iran and the international community must be a priority. This may be a limited successor to the Joint Comprehensive Plan of Action, a broader multilateral agreement dealing with regional security or separate bilateral agreements with Iran: all would serve to reduce the current high tension.

THE THREAT: ESPIONAGE

250. MI5 defines espionage as "*the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems) ...* [i.e. it] *focuses on gathering non-public information through covert means*".[216]

Intent and capability

251. In 2020, the Intelligence Community have assessed Iranian espionage to pose a significant threat to the UK and its interests, with each of the main organisations within the Iranian Intelligence Services (IIS) – the Ministry of Intelligence and Security (MOIS), Islamic Revolutionary Guard Corps Intelligence Organisation (IRGC-IO) and IRGC Quds Force (IRGC-QF) – engaging in it. Until the recent sharp increase in the Iranian physical threat (as described earlier), espionage had been consistently viewed as the most severe Iranian threat to the UK.

252. The JIC Chair told the Committee:

> *there is a significant espionage threat ... we are a priority target ... for Iran in an espionage sense ...* [for two main reasons] *... because they regard the United Kingdom as a particularly malevolent opponent of the Islamic Republic and, secondly, because of the role we play in nuclear negotiations and the relationship which we have with the United States, which* [Iran] *regards as being of significant interest.*[217]

Nevertheless, the UK appears to remain just below the US, Israel and Saudi Arabia as a target. However, MI5 cautions that this prioritisation could change depending on geopolitical events: for example, we were told that the UK was being increasingly targeted by Iranian cyber espionage, probably in relation to the ongoing sensitive bilateral and multilateral negotiations between Iran and the UK – such as the Joint Comprehensive Plan of Action (JCPOA) nuclear deal, the International Military Services (IMS) tank debt and the detention of dual nationals.

253. From the evidence that the Committee received, it appeared that the Iranian espionage threat is smaller in scale than that posed by China and Russia (as explored in the Committee's previous *Russia* and *China* Reports). Given that the UK is a priority target for Iranian espionage, this would appear to indicate that Iran's intent exceeds its capability. MI5 explained that:

> *we have in the past seen examples of espionage cases on the Iran side but we don't see anything like the same scale and breadth of targeting and it is not just* [a] *numbers game, it is not just that they have more people, it is the breadth of* [the] *Chinese, in particular, state ambition and interest across politics, economy, society, every aspect of UK life and our allies and it is just vastly different to*

[216] 'What is Espionage?', MI5 website, accessed on 25 April 2023.
[217] Oral evidence – JIO, *** June 2023.

> *Iran, where they are very focused on internal security ... regime stability and nuclear. It is a narrow set of interests ***.*[218]

The JIC Chair agreed, stating:

> *In relation to the United Kingdom, I regard the Iranian espionage threat as *** below that of Russia or China, who have longstanding, very highly funded, very technically capable, very large intelligence services and for whom the United Kingdom is, if not in their very first line of* [targets]*, close to it. Iran does have an interest in the UK but the threat to Iran does not particularly emanate from the United Kingdom ... It has a range of targets and it is *** interested in its region ***.*[219]

254. Nonetheless, Iran's espionage capability should not be underestimated. The Intelligence Community told the Committee that the IIS are capable espionage actors. The Foreign Secretary agreed, emphasising that the IIS are "*credible and capable ...* [they] *regard us as one of their top targets internationally. They are not as capable as some other threats that we face but we should not underplay the risk in any way.*"[220] It is also possible that the threat will increase over time as Iran seeks to improve its capabilities.

Purposes and targets

255. During our Inquiry it was clear that, whilst some sectors are more commonly targeted by the IIS than others, the Iranian espionage threat may not necessarily follow a set strategic plan. Director General MI5 told the Committee that *** [there are] *opportunistic attempts to gather information ... we couldn't rule out almost any sector potentially falling victim to some piece of opportunistic Iranian targeting ***, so in that sense the potential threat surface is really quite wide. Much of the time it doesn't appear to be ***.*"[221]

256. As a result, the potential espionage threat is significant in that almost any sector is vulnerable to opportunistic activity. For example, the US Department of Justice publicly reported that the Mabna Institute – an Iranian cyber organisation which does not necessarily work for one state unit but has been linked to the IRGC – conducted a co-ordinated campaign of cyber intrusions against computer systems belonging to 144 US universities, 176 universities across 21 other countries, 47 US and foreign private sector companies, US government institutions and the UN (representing one of the largest state-sponsored hacking campaigns prosecuted by the US Department of Justice). This campaign included the successful targeting of approximately 8,000 academic email accounts across the world – including in the UK – and the theft of 31.5 terabytes of academic data and intellectual property.[222] Whilst this targeting may be for a wide range of purposes – including private extortion – its activity is probably driven primarily by Iranian state requirements (i.e. it is unlikely that the Iranian government would be completely unaware, or disapproving, of its campaigns).

[218] Oral evidence – MI5, *** June 2023.

[219] Oral evidence – JIO, *** June 2023.

[220] Oral evidence – Foreign Secretary, 6 July 2023.

[221] Oral evidence – MI5, *** June 2023.

[222] ***

257. In terms of the sectors that Iran does target, the Intelligence Community told the Committee that the IIS focus on the targeting and monitoring of dissidents and other individuals considered to be a threat to the Iranian regime. Other priority targets in the UK include HMG (officials and Parliamentarians), the defence sector, academia and airlines. By way of illustration, from ***, of those cyber incidents reported to the National Cyber Security Centre (NCSC), *** were the top UK sectors targeted by Iran. From ***, the top targeted sectors in the UK were ***.

(i) Targets: dissidents and other individuals of interest

258. Director General MI5 explained that Iran's human espionage operations are targeted at: "*regime survival, dissidents* [and] *media organisations ... it is espionage of individual people who* [Iran] *perceives as being problematic for the regime ... most of the espionage activity ...* [is] *activity in support of potential future physical threat or other forms of coercive action*."[223] GCHQ told the Committee that the same is true in relation to cyber espionage, telling us: "*we particularly do see them targeting UK residents that in some way are connected to the regime's survival, so whether that be dissidents or journalists or others*".[224]

259. This focus is unsurprising given that the Iranian regime's primary objective is to preserve the regime and therefore silence critics – including in the UK. Potential IIS targets include: Iranian dissidents; journalists; individuals convicted of terrorism offences in Iran; activists; former government employees; environmentalists; refugees; university students; and employees at international non-governmental organisations. MI5 also noted that it sees Iranian espionage activity directed towards Israeli or Jewish entities in the UK, in order to pre-position and prepare for any hostile activity required by the Iranian regime.

260. Iranian cyber actors focus on targeting the airline and travel industry due to the bulk data available which can be used for intelligence and counter-intelligence purposes. This includes targeting IT companies which serve the travel sector. It is almost certain that this information is used for a range of purposes, including identification of perceived dissidents and opponents. This data could likely be used to facilitate forced repatriations or assassination attempts.

261. In relation to the Iranian focus on the aviation sector, MI5 said: "*the most interesting aspect of that has been the Iranians seeking to *** … to be able to then *** for their own *** purposes*". GCHQ echoed this, noting: "[The IIS's] *interest in *** … they recognise the power of *** and then doing … detailed analysis for *** and other purposes*".[225]

262. The IIS's analysis of bulk data demonstrates a particular level of sophistication and capability, even though this may not be on the same scale as Russia and China. As Director General MI5 said: "*they are not crude in a lot of what they do, their counter-intelligence work is *** and certainly we know of a ****".[226]

[223] Oral evidence – MI5, *** June 2023.
[224] Oral evidence – GCHQ, *** June 2023.
[225] Oral evidence – GCHQ, *** June 2023.
[226] Oral evidence – MI5, *** June 2023.

Targeting of travel information

APT39 is an Iranian cyber espionage group, active since at least 2014. It has been linked to a front company, Rana Intelligence Computing (Rana), which the US Federal Bureau of Investigation (FBI) has publicly linked to MOIS. APT39 has shown a particular interest in the transport sector (as well as other sectors) and is renowned for its focus on stealing bulk personal datasets from organisations across the world. It is likely that its primary remit is to use personal datasets to enable monitoring, tracking or surveillance operations in support of Iranian government objectives.

PwC, the professional services firm, identified a purported list of airlines which it is likely that APT39 actors planned to target – including 40 airlines based in Asia, the Middle East and North America. This list suggested that at least 13 out of the 40 airlines were successfully targeted. In 2020, the US Treasury Department sanctioned APT39 and Rana as well as 45 associated individuals for undertaking a "*years-long malware campaign that targeted Iranian dissidents, journalists and international companies in the travel sector*".[227]

(ii) Targets: HMG

263. Gathering information on HMG (including the Intelligence Community) is a key objective for Iran in relation to the UK, to help protect the Iranian regime and respond to UK activity relating to Iran. For example, understanding the strategy of other states – such as the UK – on nuclear negotiations is presumably a priority for the IIS and the broader Iranian regime.

264. We were told that Iranian cyber actors had previously targeted personal email accounts of former and serving members of the UK Civil Service, military and Parliament, presumably seeking to acquire information relating to HMG policy and intent ***. Similarly, Iranian cyber actors have previously targeted several UK Government entities, including ***.

265. In order to gather information on HMG and the Intelligence Community, the IIS are interested in a broad range of profiles. They seek to exploit anyone whom they judge would be able to provide them with access – even occasional – to information, even if it is unclassified. As it is highly likely that the IIS aspire to recruit members of staff working on Iran-related issues, staff working at the Foreign, Commonwealth and Development Office (FCDO), Ministry of Defence (MoD), Home Office and Cabinet Office are all targets of interest.

266. Given the capability of the IIS, the Committee questioned whether the IIS were able to penetrate the UK Intelligence Community or foreign intelligence services. MI5 told us that ***. As the Chief of SIS told us: "*They* [the IIS] *are very good and very professional *** So I wouldn't underestimate them for a minute*". Director General MI5 told us:

> ***.[228]

[227] 'Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry', US Department of the Treasury, 17 September 2020.

[228] Oral evidence – MI5, *** June 2023.

Targeting of HMG

British Army: Daniel James was a dual British-Iranian national who served in the British Army as a reservist. He served as an interpreter to Lieutenant General David Richards in 2006, who at the time was the Commander of NATO Forces in Afghanistan. General Richards had access to sensitive information of strategic value to Iran and James had direct access to him through his interpreter role. An investigation into James concluded that he was being managed by an IIS intelligence officer, who was probably affiliated with the IRGC and was based at the Iranian Embassy in Kabul. It is likely that James was financially motivated to pass sensitive information to the IIS and volunteered himself to them as an asset. He was subsequently arrested and jailed for ten years for breaching the Official Secrets Act.

*****:** In ***, MI5 issued an 'Espionage Alert' to Whitehall departments regarding the activities of a UK-based *** national who was an agent of the IIS. He had previously been employed at ***, and, after relocating ***, later obtained employment at ***. After leaving ***, the individual maintained a relationship with ***. Whilst it is highly unlikely that the individual was able to exploit the access to obtain classified information, he may still have obtained information of interest to the IIS.

*****:** In ***, MI5 issued an 'Espionage Alert' to *** in relation to a UK-based *** identified as an IIS agent who had ***. This allowed the individual to engage *** on topics that likely were of interest to the IIS.

(iii) Targets: regional networks and multilateral organisations

267. Iran's targeting of regional networks and multilateral organisations – and in particular the activity of Iranian cyber groups in the Middle East – poses a risk to UK data held abroad, given the multinational and interconnected nature of industry and networks.

268. According to the Intelligence Community, the IIS employ espionage in the Middle East ***. It is highly likely that the IIS's ability to obtain UK-related information from *** regional networks ***.

269. As such, the Intelligence Community have concluded – as far back as 2016 – that ***. ***, the IIS had targeted regional governments presumably for the purpose of gathering intelligence to support Iran's regional and global diplomacy. ***.

270. Iran has also targeted the networks of international organisations such as the UN. For example, in 2018, the US Department of Justice reported that an Iranian cyber actor had targeted UN networks, including the United Nations Children's Fund (UNICEF). In 2022, intelligence reporting indicated that ***. The IIS almost certainly are interested in the activities of the International Atomic Energy Agency (IAEA), including its monitoring of Iranian nuclear facilities, so it is highly likely that they undertake activity against the IAEA and its inspectors ***.

271. The collateral threat to the UK from ‘third-party’ targeting can be significant. For example, according to public cyber security reporting, in 2022 Iranian state-linked actors reportedly exfiltrated data from an Israeli defence company, which also allowed them to obtain data relating to a UK purchase of a ground-based air defence system. As such, the Committee was told that, when engaging with governments and intelligence agencies ***, the Intelligence Community ***

(iv) Targets: academia

272. Iran almost certainly conducts espionage campaigns targeting academia and the research sector around the world, including academics, think tanks and policy experts. While targeting may be opportunistic, many of the attacks are successful – for example, in 2020 Iranian cyber actors had compromised various UK academic and civil society organisations by setting up fake login pages.

273. Whilst the motivation for undertaking espionage operations against academics and educational organisations varies between cyber groups and can be difficult to identify, NCSC told the Committee that the most likely reason is to steal intellectual property, as well as scientific and research information. This activity includes the electronic theft of academic materials which are then translated into Farsi and sold to Iranian universities and other government organisations.

274. Iranian cyber actors also target the academic sector so that they can then use the sector’s often poorly defended networks as platforms through which to facilitate attacks on other organisations. In any given case, the targeting may also be less related to potential intellectual property or cyber pre-positioning and more linked to the views of the individual academic, i.e. targeting dissidents who are also academics or who have connections with Iranian dissident groups.

Targeting of nuclear information

In 2021, NCSC confirmed that Iranian cyber groups – known as the Mabna Institute and CHARMING KITTEN – had targeted a range of academic sources which almost certainly would have included sources with nuclear-related information.

The **Mabna Institute** was founded in 2013 and initially focused on targeting intellectual property via cyber espionage. As previously noted, it has been linked to the IIS. The US Department of Justice reported that it previously sponsored a four-year campaign targeting universities to gain access to academic and intellectual property.

CHARMING KITTEN is an Iranian cyber espionage group that has been active since at least 2014. It is believed to have targeted a range of sectors, including US and UK universities and think tanks, academics, and organisations focused on conflict resolution. Through this targeting, the group sought to gain insight into and influence international policy positions on the Iranian nuclear deal.

The targeting of technical nuclear information is probably less of a priority for the IIS in the UK given the advanced state of Iran's nuclear programme, although acquiring further nuclear know-how may well still be desirable. The IIS also highly likely continue ***.

(v) Targets: defence

275. Given Iran's strategic objective to maintain the security of the regime, it focuses on intellectual property theft in the defence sector. GCHQ explained:

> [its targeting] *still does flow from the strategic objectives ... regime survival being the primary one, so the area where they do try and get information which might be considered to be intellectual property theft first and foremost are things like the defence sector. So for their survival, clearly the development of Iranian indigenous weapons systems is really important, and therefore *** cyber means to target defence companies ... ***.*[229]

276. Iran's targeting of the defence sector could help it to develop its own defence capability or to understand the defence capability and activity of foreign adversaries active in Iran's near abroad. This potentially provides Iran with a strategic advantage. It may for example reduce the impact of international sanctions that have been imposed on Iran's weapons programmes. It may also provide Iran with a greater understanding of UK defence capabilities, particularly those exported to the Middle East region. In the broadest terms, this serves to support Iran's objectives of containing the West, becoming a leading regional power and, ultimately, preserving the regime.

277. GCHQ explained that the scale of intellectual property theft is significantly smaller when compared to China: "*it is very different to the Chinese IP threat ... partly because of scale, partly because ... the Chinese ability to convert that high-end intellectual property into economic ... science and technology advantage is much greater than the Iranians*".[230]

278. The Committee was told that the cyber espionage threat posed by Iran to UK defence, including the defence industry, had almost certainly grown in recent years (although the UK is probably not Iran's top priority). As Iranian cyber actors regularly target UK allies, this additionally presents an indirect threat to UK defence interests ***.

(vi) Targets: healthcare

279. Following the impact of the global pandemic on Iran, Iranian cyber actors targeted the healthcare sector almost certainly in order to understand how the pandemic was affecting other countries and how they were responding, as well as to support its own response, including vaccine development. For example, ***

[229] Oral evidence – GCHQ, *** June 2023.

[230] Oral evidence – GCHQ, *** June 2023.

(vii) Targets: UK Critical National Infrastructure

280. The Intelligence Community have previously judged that Iran was conducting espionage against UK Critical National Infrastructure (CNI) (***). From the evidence we received, it appears to pose a very significant state threat to UK CNI, alongside *** the threats from Russia and China which we have considered in previous reports. This could be for a variety of purposes – for example, seeking commercial or military information, or for counter-intelligence purposes.

281. Nevertheless, it may not be a top priority for the IIS (unlike, for example, information on UK-based Iranian dissidents and HMG). Any Iranian cyber incidents targeting UK CNI could be opportunistic or for espionage purposes ***. The Committee questioned whether there was any major risk to UK CNI from Iranian investment – given that Iranian investment in the UK's CNI is relatively small, partly limited by the international sanctions on Iran. The Intelligence Community told the Committee that ***

Using human sources

282. The IIS will seek to use individuals in the UK to acquire information on targets, running them as agents while their case officers remain located outside the UK. *** to use a UK-based agent to help facilitate a relationship with an individual of interest. (Generally speaking, it is not necessarily a hindrance for a foreign agent-handling intelligence officer to be based outside of the UK as intelligence services often use other people *** to transport items and intelligence, and case officers can debrief their agents abroad where the operating environment is more permissive than in the UK.) ***

283. Examples of IIS agent profiles include journalists, academics, religious figures and students, including those linked to reputable organisations. In particular, the IIS have targeted the following groups for recruitment:

- individuals who regularly travel to the Middle East, dual nationals, and Iran-based family members and associates of targets;
- Farsi-language students and who may go on to work in sensitive areas; and
- current and former foreign government officials, including intelligence officers.

We consider these in more detail below.

(i) Individuals who regularly travel to the Middle East, dual nationals, and Iran-based family members and associates of targets

284. Individuals who regularly travel to Iran or near Iran are often attractive targets for the IIS – including those who are dual-nationals or those with familial links to Iran or someone who has ethnic or religious ties to Iran or the region. The IIS may also try to identify, target and recruit British nationals travelling in Iran for the purpose of conducting long-term

'seeding' operations against HMG: Director General MI5 told the Committee that the IIS are interested in "*long-term operations to 'seed' in relatively junior people to start penetrating* [HMG's] *system*[s] *who would have long-term access and benefit for them*".[231]

285. The IIS use coercive tactics to force family members to co-operate and support their recruitment aims. It is therefore highly likely that family members of HMG and Intelligence Community staff who live in or travel to Iran – or areas where the IIS are comfortable operating – face an increased risk of interrogation and recruitment if the staff member's employment becomes known.

286. The IIS monitor visitors to Iran as they cross the border via land, sea and air routes. The IIS interview Iranians – including dual-nationals – overtly as intelligence officers and ***. It is highly likely that the information obtained is used to inform their targeting and recruitment work and, where individuals of interest are identified, they may be added to a travel notification system.

287. The IIS are also likely to intercept international calls to and from Iran to support its espionage operations, ***. For example, in ***. That information is highly likely to help support counter-intelligence investigations as well as agent recruitment operations.

(ii) Farsi-language students

288. Despite the focus on those with links to Iran, it is also likely that the IIS target other individuals (for example, British nationals) if the opportunity arises and they have access to useful information. This even includes those who may potentially have access to useful information in the future (even if they had little intelligence value at the time that they were recruited). Director General MI5 told us:

> *We have seen examples where the Iranians have sought, either in Iran itself or in third countries, ... to recruit comparatively junior people, students, people who don't today have any access to privileged information but who might get there. So they are patient and up for trying to do ... seeding type of operations where they cultivate people who might be a bit more naive, or early in their careers with a view to then becoming longer-term assets.*[232]

289. An example of such a target would be British nationals studying Farsi, given the possibility that they may subsequently work on Iran-related issues. ***. Nonetheless, the IIS are more likely to target individuals who travel to or study in Iran or in a country where the IIS are able to operate more freely, than those who study in the UK. One example is the ***.

[231] Oral evidence – MI5, *** June 2023.

[232] Oral evidence – MI5, *** June 2023.

***

***

This scenario demonstrates that the IIS seek to use their global presence to identify recruitment targets, and it is likely that the IIS target other students whom they judge to have the potential for future access to security, government and international institutions (such as the UN, EU and NATO), particularly where the IIS have a presence and are comfortable operating, for example ***.

It is possible that IIS officers posted overseas could develop relationships with local Farsi-language schools in order to identify recruitment targets. *** this could be for the purpose of counter-intelligence or espionage.

(iii) Current and former foreign government officials

290. Given that the IIS prioritise targeting HMG to gain access to sensitive UK Government information, it is not surprising that they aim to recruit current and former government officials who are working on, or have previously worked on, Iran-related issues. As the Committee's *China* Report reported, foreign intelligence services use various methods for recruitment attempts, including social media such as LinkedIn.

291. Reporting shows that the IRGC has also used international conferences in Iran to engage, target and recruit foreign nationals, in particular former foreign government officials such as members of parliament, military personnel, intelligence officers and civil servants. A key example is the 'New Horizon' Conference used by the IRGC, which is explored below.

New Horizon Conferences

The New Horizon Organisation has organised several international conferences in Lebanon and Iran. It is almost certain that the IRGC uses New Horizon Conferences as an opportunity to gain access to and recruit foreign nationals as agents.

Previous attendees have included a former US State Department official, a former US Army psychological operations officer, former US Intelligence Community case officers and a European member of Parliament.

In 2012 and 2013, US national Monica Witt, a former US Air Force cryptologist and counter-intelligence officer (as well as a former analyst for the defence contractor, Booz Allen Hamilton), travelled to several New Horizon Conferences in Iran. During these trips, she revealed the existence of a classified intelligence collection programme and the true identity of a US intelligence officer. In late 2013, Witt is believed to have defected to Iran where she has provided support to the IIS by conducting research on her former colleagues.

Witt's case shows the risk of former members of government staff and demonstrates that the IIS continue to target individuals even where they may no longer maintain current access to classified information.

In 2019, the US government sanctioned the New Horizon Organisation for its support to IRGC-QF in providing a platform for IIS intelligence officers to recruit and collect intelligence from attendees of its conferences, including foreign nationals (as well as propagating anti-Semitism and Holocaust denial).

292. The IIS are also likely to attempt to use 'double agents'[233] to obtain information relating to the activities of foreign intelligence services, including the UK Intelligence Community. For example, in 2019 MOIS revealed the identities of several alleged US Central Intelligence Agency (CIA) officers working on Iran-focused operations. This included images and recordings of alleged CIA officers ***. The IIS have also demonstrated their ability to penetrate the German Armed Forces ***.

(iv) State-linked institutions overseas

293. It is likely that the IIS use state-linked institutions to identify and recruit targets – for example, the Islamic Centre of England (ICE) and the Iranian Embassy. The ICE, based in London and with sub-branches in Birmingham, Newcastle, Glasgow and Manchester, is the UK's largest Shi'a cultural and religious educational centre. The centre is largely funded by the Supreme Leader's Office and its director is the Supreme Leader's religious representative in the UK (and is personally appointed by the Supreme Leader). Its activities include conferences, seminars, lectures, magazines and religious events, predominately in London. This includes political activities, such as holding a candlelit vigil following the US killing of IRGC-QF Commander Qasem Soleimani in 2020.

294. Given the close links with the Iranian state, the ICE may well provide IIS agents with a useful base from which to act. ***.

295. When the Committee questioned the Intelligence Community about ICE, ***. We return to the potential threat posed by ICE in the 'Interference' chapter.[234]

296. We also questioned whether the IIS use the Iranian diplomatic mission to conduct espionage activity. We were struck by the assessment that ***. Director General MI5 told us:

> ***[235]

[233] A 'double agent' pretends to act on behalf of one country or organisation when in fact acting on behalf of an adversary.

[234] Oral evidence – ***, *** June 2023.

[235] Oral evidence – MI5, *** June 2023.

Using technical means

297. During our Inquiry, we heard that the Iranian espionage threat manifests acutely in the cyber domain. UK entities are regularly targeted by Iranian cyber organisations for the purpose of intelligence and counter-intelligence. Iran often uses cyber espionage as it is cheap, deniable, and enables the IIS to gain information which would often not be possible to obtain within countries – such as the UK – due to the difficult operating environment. Given the focus on using technical means to conduct espionage, we consider this separately in the following chapter.

FF. Iran poses a significant espionage threat to the UK and its interests, projected primarily via cyber capabilities, but also via human agents. Whilst as a target, the UK appears to remain just below the US, Israel and Saudi Arabia, this prioritisation could change depending on geopolitical developments and the relationship between Iran and the UK.

GG. The espionage threat is focused on supporting Iran's primary objective of regime stability: it is substantially narrower in scope and scale, and less sophisticated, than that posed by Russia and China. In the UK, the Iranian Intelligence Services prioritise targeting opponents of the regime, HMG and sectors that may provide the Iranian regime with a strategic advantage such as academia and defence. However, the Iranian espionage threat may not necessarily follow a set strategic plan – there is more of an opportunistic element in its targeting.

HH. There is a collateral threat to the UK associated with Iran's targeting of regional networks and multilateral organisations. Given Iran's focus on the Middle East, Iranian cyber actors in the region are particularly active. This increases the risk to the UK if it were to share sensitive data with those whose networks may be a target of the Iranian Intelligence Services.

II. While both the Iranian Embassy and the Islamic Centre of England have legitimate roles supporting the Iranian diaspora community, given their close links to the Iranian regime they are also likely to provide a permissive environment for Iranian Intelligence Services agent recruitment and intelligence gathering in the UK. We encourage the Intelligence Community not to underestimate the potential espionage threat they pose.

THE THREAT: CYBER ENVIRONMENT AND CAPABILITIES

298. Over the last 15 years, Iran has developed proficient cyber skills: as the Home Secretary told us, Iran is a "*capable and aggressive cyber actor*".[236] It has extensive cyber capabilities which it uses to meet the regime's intelligence requirements and to damage adversaries. Whilst *** Iran does not possess the same sophisticated cyber capability as Russia and China. (As described in the Committee's previous *Russia* and *China* Reports, both Russia and China are highly capable, effective and sophisticated cyber actors, whose cyber expertise allows them to target a range of sectors and organisations.) We note the report by the Carnegie Endowment for International Peace that Iran lacks the capability of Israel and the US, ***. HMG described Iran as:

> **** not to be underestimated, the level of threat that the Iranian cyber capabilities represent and particularly when associated with that higher risk appetite, but at the moment the combination of intent and capability does not put them in the same level as we perceive from Russia and China.*[237]

299. This chapter will explore Iran's cyber capabilities and the complex Iranian cyber landscape, including how the Iranian Intelligence Services (IIS) co-ordinate cyber activity. (We will explore how Iran uses its cyber capabilities for the purpose of disruptive and destructive effect in the next chapter.)

Iranian cyber environment

Formative experiences

300. Between 2010 and 2012, Iran suffered a series of significant offensive cyber-attacks on its critical infrastructure, from malware known as 'Stuxnet' (2010) and 'Wiper' (2012). Given the damage they caused, they had a defining impact on Iran and almost certainly motivated it to develop its own offensive and defensive cyber capabilities, including in relation to espionage and Industrial Control Systems (ICS).[238] The 'Wiper' attack in particular provided a blueprint for Iranian cyber actors to replicate.

[236] Oral evidence – Home Secretary, 6 July 2023.

[237] Oral evidence – HMG, *** June 2023.

[238] Industrial Control Systems are hardware and software used in the operation of industrial processes, such as in Critical National Infrastructure.

Stuxnet and Wiper attacks

Stuxnet was a form of malware – i.e. malicious software – that spread to at least 14 industrial sites in Iran, including the Natanz nuclear facility. Media reporting claimed that up to 1,000 of Iran's centrifuges were destroyed by this malware (by overriding ICS). Media reporting suggests that this attack was jointly developed and co-ordinated by Israel and the US National Security Agency in an effort to slow Iran's nuclear programme.

Wiper was another form of malware targeting Iran's oil and gas industry, oil ministry and other affiliated organisations. It destroyed data and rendered much of the sector's infrastructure inoperable. Unlike Stuxnet, Wiper was replicable and the National Cyber Security Centre (NCSC) assesses that it highly likely enabled Iran to develop its own cyber offensive capability.

Current environment

301. IIS work on cyber is a complex picture, incorporating an extensive network of state institutions and private enterprises. NCSC described the Iranian cyber landscape as:

> *an ecosystem made up of cyber groups that can be categorised on a spectrum between state institutions such as MOIS* [Ministry of Intelligence and Security] *or the IRGC* [Islamic Revolutionary Guard Corps] *and those that are private organisations showing very little state affiliation. Other groups exist in the grey area between these two extremes: private groups that do not belong to state institutions, but with varying degrees of state links and state control.*[239]

302. According to NCSC, the greatest threat is posed by cyber actors that belong to the IIS as they will be under direct state control. However, in addition to state-affiliated actors, private cyber actors also pose a threat, operating to either known or perceived state intelligence requirements. Whilst some private cyber actors respond to direct state tasking and have formal government contracts, others conduct cyber criminal activity for their own financial gain, and some conduct opportunistic activity that falls broadly within state intelligence requirements.

303. Each Iranian cyber group has different characteristics but – in respect of the UK and its Western allies – they share a primary focus: to conduct cyber activity against a range of targets. This enables: intelligence gathering; disrupting those whom Iran considers a threat to the regime; developing influence operations; and undertaking offensive cyber-attacks to project power and to respond to perceived slights and geopolitical events.

304. The complexity of the Iranian cyber landscape appears to make it more difficult to determine accurately the motivation behind Iranian cyber targeting and the level of Iranian state control. GCHQ told the Committee that there are:

[239] Written evidence – NCSC, 16 January 2018.

> *state-affiliated groups ... which are clearly given a remit *** a certain framework, for example ***, and ... some **** ... [there are also] *** *activities by different cyber organisations ... against *** targets ... *** ... there are cyber actors associated with Iran who both conduct activity on behalf of the Iranian state either because they have been directed or because they perceive that is what the Iranian state would like and they might benefit from that* ... [they] *do it in order to get personal gain.*[240]

Co-ordination between cyber groups

305. It was previously assessed that the Iranian cyber effort consisted of disparate groups ***

306. The individuals in these cyber groups – consisting of either contractors or employees (for example working in departments within the IIS) – ***. Whilst the fluid nature of Iran's cyber landscape may result in increased flexibility, deniability and unpredictability, equally it is possible that fluidity could undermine its effectiveness.[241]

Cyber support to Iranian-aligned militant and terrorist organisations

307. In addition to this complex cyber landscape, Iran has almost certainly contributed to the cyber capabilities of some of the militant and terrorist organisations in the Middle East with whom it has relationships. As noted in cyber security industry reporting, Iran has provided cyber assistance to Lebanese Hizbollah and Hamas. The value of Iran's assistance can be seen in the Intelligence Community assessment that Lebanese Hizbollah has the highest cyber capability of any terrorist group.

Cyber tools and techniques

308. The Intelligence Community explained that the tools and techniques Iran uses to conduct computer network exploitation might often be basic but they are used very effectively. GCHQ told the Committee: "*one of the reasons Iran is successful is not because they are highly sophisticated but because they can exploit fairly basic vulnerabilities that still too many organisations in the UK have*".[242] For example, Iranian cyber actors are proficient in their use of targeted techniques such as 'social engineering' and 'spear-phishing', which they use to gain credentials that confirm an individual's identity and to deploy malware, whilst also using untargeted methods such as 'password spraying' to gain access to networks and accounts.

309. The unrestricted way in which Iranian cyber actors are able to operate appears to exacerbate the cyber threat. GCHQ explained: "*the Iranians will often go after* [cyber] *targets without any kind of ethical concerns* ... [they don't have] *the same good process*[es] *as we have to ensure our operations are legal and proportionate and necessary*".[243]

[240] Oral evidence – GCHQ, *** June 2023.

[241] ***

[242] Oral evidence – GCHQ, *** June 2023.

[243] Oral evidence – GCHQ, *** June 2023.

Obtaining bulk personal datasets

310. This technique involves obtaining and analysing extensive datasets – for example, from airlines, hotels or other travel companies. NCSC said that increasingly proficient Iranian cyber actors aim to streamline such operations for maximum return and to maintain long-term access to such targets.

Compromise of **

In ***, NCSC assessed that a *** had been compromised almost certainly by a cyber group linked to the IIS. The group focuses on the extraction of bulk personal data which it almost certainly uses to identify foreign intelligence officers and their agents and to track Iranian dissidents.

Password spraying

311. Iranian cyber groups use 'password spraying' to access networks or online accounts. This involves using a set of common passwords to attempt to access a large number of accounts. They are often successful because for any given large set of users there will be a proportion who use very common passwords.

Compromise of UK Parliament

In 2017, the BBC reported that UK civil servants had accused Iran of being responsible for a major cyber-attack on Parliamentary email accounts, including those of Cabinet Ministers. ***. 200,000 attempts were reportedly made to target 9,000 email accounts and 39 email accounts were reportedly compromised – including the inbox of six MPs and ten MPs' staff. This cyber-attack caused significant disruption, requiring the Parliamentary authorities to temporarily restrict remote access to the Parliamentary network.

According to reports, Iranian-linked cyber actors used a 'password spraying' technique. ***

At the time of the incident, ***

We asked the Intelligence Community whether there had been Iranian attempts to target the UK Parliament since 2017. GCHQ told the Committee that ***.[244]

Social engineering and spear-phishing

312. Social engineering refers to the manipulation of people into carrying out specific actions such as divulging information that is of use to a cyber actor. Spear-phishing involves

[244] Oral evidence – GCHQ, *** June 2023.

sending targeted emails asking for sensitive information or encouraging targets to visit a fake or compromised website. Both techniques are used by Iran-linked cyber actors to gain access to sensitive information.

Case studies: spear-phishing and social engineering

Journalists – As noted above, CHARMING KITTEN is a cyber espionage group that has been widely linked to the Iranian state and has been active since at least 2014. NCSC has assessed that it poses a *** cyber espionage threat to a variety of sectors including HMG, gathering intelligence in support of Iran's ***. It often uses social engineering and spear-phishing techniques to access information. This has included using the identity of current and former journalists from international publications such as the Wall Street Journal, CNN and Deutsche Welle. The approaches lure the target onto the cyber group's websites which appear to be legitimate email or social media accounts. This then enables the group to collect the target's passwords and login credentials, allowing it to access information and target further individuals and accounts.

In 2019, Microsoft filed a complaint with the US District Court for Washington D.C. against CHARMING KITTEN for establishing a series of domains that mimicked login pages for Yahoo!, LinkedIn, Hotmail, Microsoft Live and other services.

*** – In another example of this type of activity, between ***, CHARMING KITTEN undertook 'spear-phishing' operations in which it impersonated the ***. The operation also targeted an employee of another UK-based *** and *** officials.

CHARMING KITTEN has been known to target activists, defence contractors, academia, government agencies, media organisations, and companies in the financial, energy and aerospace sectors. *** its targeting of UK politicians and civil servants. It has also *** targeted individuals resident in the UK, including those whom Iran perceives as a threat to the regime such as activists. Following the outbreak of the Covid-19 pandemic, the group targeted individuals *** linked to the healthcare sector, reflecting changes that were likely made to its and other Iranian cyber groups' intelligence requirements.

***** Embassy** – CARDAMOM is a cyber group linked to the IIS's ***. In ***, it compromised the account of the *** at the *** Embassy in *** through the use of *** spear-phishing message. The group was able to obtain several emails from this account that had been received from a ***, demonstrating the potential risk of *** data being taken from third parties.

Artificial Intelligence

313. We asked whether the cyber threat from Iran had increased due to the greater interconnectivity of technology and developments in Artificial Intelligence (AI) technologies. The Foreign, Commonwealth and Development Office noted that Iran is already using generative AI for operational use and that the Supreme Leader had referred to the development

of AI as a requirement. AI has been used in Iran, including in relation to the evolution of security systems such as: facial recognition; intelligent weapons; intelligent robots and devices for use in manufacturing and industry; and speech recognition.

314. GCHQ recognised the threat of technology development, telling us:

> *The greater interconnectivity means the risk of spillover from a cyber operation into an unintended or indirect target is ... potentially increasing ... Artificial Intelligence* [also] *improves your ability to get value of out of data. It, equally, can be used to help protect networks as well ... but* [it] *is definitely a factor, yes.*[245]

315. The Foreign Secretary also noted the threat of AI:

> *The amplifying effect of AI is one of the things that ... right across the board we have to be very, very conscious of. It makes it ... cheaper and easier for them and it makes it harder for us, and we need to respond to that.*[246]

JJ. Iran is an aggressive cyber actor with extensive capabilities. Whilst Iran does not possess the same sophisticated capability as Russia and China, the cyber threat posed by Iran is significant.

KK. The Iranian cyber threat landscape is complex, with cyber groups ranging from state-controlled actors responding to direct tasking, to private cyber actors working for personal gain or perceived state intelligence requirements. The complexity of this environment appears to make it more difficult to identify accurately the motivation behind Iranian cyber activity and the level of state control.

LL. Whilst Iranian cyber actors often use simple computer network exploitation techniques, they use them very effectively, exploiting basic vulnerabilities that many organisations have, including in the UK. They do this for the purpose of gathering intelligence, undertaking interference operations and enabling offensive (disruptive and destructive) cyber operations.

MM. The ever-increasing interconnectivity of global technology and developments in Artificial Intelligence may exacerbate the Iranian cyber threat.

[245] Oral evidence – GCHQ, *** June 2023.

[246] Oral evidence – Foreign Secretary, 6 July 2023.

THE THREAT: OFFENSIVE CYBER

316. ‘Offensive cyber’ is usually used to describe any hostile cyber activity, whether it is used for espionage or to destroy or disrupt IT systems. Since cyber espionage has been covered in previous chapters, in the context of this chapter ‘offensive cyber’ will be used to refer just to the use of destructive or disruptive cyber-attacks that are intended to destroy or disrupt IT systems. We consider below Iran’s objectives, capability, intent and the sectors it is targeting.

Objectives

317. According to the Intelligence Community, there are two broad drivers for Iranian offensive cyber operations:

- projecting strategic power; and
- responding to perceived slights or acts of aggression or geopolitical events.

Once again, these drivers reflect Iran’s overarching objectives of maintaining its position as a leading regional power and containing its regional and global adversaries, which are viewed as essential to ensure the safety and security of the regime.

318. As explored in the chapter on Iranian cyber capabilities, a key motivation behind Iran’s development of an offensive cyber capability was the series of significant offensive cyber-attacks on Iranian critical infrastructure, which took place in 2010 (Stuxnet) and 2012 (Wiper). However, it has also been driven by Iran’s preference for a proportionate response (as previously noted, responding in a similar way to perceived aggression). As such, a response is not always achievable or realistic given the military superiority of Western forces and Iran’s geopolitical isolation; Iran has developed asymmetric capabilities – and offensive cyber is a good example of just such a capability. As Professor Ehteshami explained:

> [offensive cyber is] *part of* [Iran’s] *asymmetrical warfare strategy* ... [it is] *something they are increasingly able to use offensively* ... [but] *what drives them still is this notion of deterrence, that we* [i.e. Iran] *must stop them* [i.e. the West] *or we must make them not do things to us by virtue of acquiring the means to test their resolve.*[247]

319. Offensive cyber not only allows Iran to attack and contain Western and regional adversaries without resorting to conventional military action, it also provides Iran with a deniable tool and one which gives it a clear advantage in the region ***.

Iranian capability

320. As the chapter on Iranian cyber capabilities explored, Iran is an aggressive and capable cyber actor, which is reportedly likely to be capable of using offensive cyber operations to cause major disruption in the Middle East but also in the UK (although Iran’s offensive cyber

[247] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

capability remains behind that of Russia and China). As a result, if the requisite Iranian intent to undertake such activity existed, the National Cyber Security Centre (NCSC) assesses that UK entities would almost certainly be targeted by *** Iranian offensive cyber activity.

321. Since 2012, Iran has continued to develop and refine its offensive cyber techniques, particularly in the Middle East. As GCHQ explained:

> *The higher risk appetite has manifested itself in* [...] *disruptive attacks against regional powers, particularly Israel and Saudi Arabia over the last ten years. So* [Iran] *has been learning from those attacks and developing their methodology.*[248]

322. The previous chapter explained that Iranian cyber actors often use relatively basic tools to access IT systems, such as password spraying, social engineering and spear-phishing. Once they have access, they utilise a number of destructive and disruptive tools. Destructive 'wiper' malware attacks – which delete data and damage equipment at scale – are Iran's key destructive cyber capability, although it has also developed the capability to target Industrial Control Systems (ICS) which are used in Critical National Infrastructure (CNI) globally. Iranian cyber actors have also used 'distributed denial of service' attacks against both Saudi and Israeli websites. These send multiple requests to a website to overload it and prevent it from functioning correctly. Ransomware – which prevents access to a device, often as an attempt to extort money – is another tool used by Iranian cyber actors. Examples of these capabilities in action are provided below in the section on 'Targeted sectors'.

Iranian intent

A significant target

323. Whilst Iran is an aggressive cyber actor with a relatively high risk appetite, the offensive cyber threat from Iran is different to that posed by Russia and China: "[Iran] *does not want to ... bring the ceiling down on their heads* ***".[249]

324. It appears that the UK is not a top priority for Iranian offensive cyber activity: as such, in the current environment, Iran may not attempt an offensive cyber-attack specifically to damage the UK unless it was directly provoked (particularly as such an attack would presumably be perceived as highly escalatory by the international community, risking a significant international retaliation). Therefore, as a target, the UK appears to be behind the US, Israel, Saudi Arabia and other regional adversaries. Consequently, the JIC Chair told us: "*the threat of Iranian large-scale disruptive or destructive cyber-attacks against the United Kingdom is* ***".[250]

325. Whilst it is unlikely that Iran currently intend to launch an offensive cyber-attack directly against the UK or its interests, it is important to note Iran's capacity to prepare and position itself for future offensive cyber-attacks – Iranian cyber groups persistently scan for cyber vulnerabilities in HMG and other UK entities.

[248] Oral evidence – GCHQ, *** June 2023.
[249] Oral evidence – JIO, *** June 2023.
[250] Oral evidence – JIO, *** June 2023.

Provocation

326. The Committee was interested in what would provoke Iran to undertake an attack against the UK. As noted previously, Iran's intent to target the UK could change quickly if the bilateral relationship between Iran and the UK significantly deteriorated. This adds a layer of unpredictability to the Iranian threat as it will be influenced by regional and geopolitical developments. For example:

- The Joint Comprehensive Plan of Action (JCPOA) nuclear deal – in which Iran agreed to restrict its nuclear programme in return for the international community removing economic sanctions – very probably had a restraining influence on Iran's intent to conduct offensive cyber activity against the signatories of the deal (including the UK).
- The subsequent US withdrawal from the JCPOA may have increased the Iranian cyber threat towards the US.
- The British seizure of an Iranian oil tanker in 2019 might have led Iran to use offensive cyber against UK interests in retaliation.
- The US killing of the Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) Commander General Qasem Soleimani in 2020 might have led Iran to use cyber to retaliate – although given the UK's relatively neutral stance, the UK itself might not have been targeted.

327. The threat to the UK could change if Iran perceives the UK to have changed its position or to be responsible for a cyber-attack or aggression against Iran (even if this does not reflect reality), which is demonstrated by the below case study.

Iranian perception of UK involvement in cyber-attack

*** NCSC assesses that, if Iran perceives that the UK has been complicit in conducting offensive cyber activity against it in the future, it is likely that Iran will conduct retaliatory action against UK-associated targets – including via offensive cyber activity.

328. Although, as a target, the UK appears to be behind the US, Israel and Saudi Arabia, it is probable that Iran's intent to conduct offensive cyber activity against the UK is increasing. This is due to Iran perceiving the UK to be involved in hostile state activity against it – for example, in 2022 it was reported that the Iranian regime had accused the UK of hosting Farsi-language news outlets which Iran perceived to have contributed to the outbreak of internal protests following the death of the Iranian student, Mahsa Amini. This follows an increase in Iran's willingness to use offensive cyber in the region, driven by regional tensions and a desire to project power (as well as the lack of a direct challenge or response from its adversaries).

Thresholds

329. In 2017, the Intelligence Community judged that Iran's thresholds for using offensive cyber were *** Iran's willingness to use offensive cyber in peacetime as well as in war to influence and to punish. When we questioned the extent to which we understand how Iran's thresholds compare with other state threats, the JIC Chair told the Committee that:

> **** I would surmise that Iranian aggression against the United Kingdom would rise quite sharply if Iran thought that the United Kingdom was complicit in some attempts to undermine the Islamic Republic in some way ... Iran very often seeks to respond to what it sees as other states' aggression in what they regard as a proportionate way ...* ***.[251]

Deterrence

330. The Intelligence Community also told the Committee that, if Iran wanted to deter the UK from acting in a particular way, *** offensive cyber can be unpredictable both in relation to its inherent effectiveness and in relation to conveying a particular message.

Collateral damage

331. Even when not intending to undertake a direct offensive cyber-attack on the UK, we noted with concern Iran's willingness to accept the risk of collateral damage to the UK and its interests. Due to multinational trade and the interconnectedness of IT networks, it is likely that any global increase in Iranian offensive cyber activity increases the risk to UK entities (for example, through collateral damage resulting from broader activity against a particular sector). Further, according to NCSC, it is unlikely that all UK entities are able to detect or defend against Iranian offensive cyber activity (whether directly targeted or as collateral damage).

Key actors

*Actors: ****

332. Following the *** cyber-attack, the Iranian Intelligence Services (IIS) established a new cyber actor, ***. According to NCSC, ***.

333. According to the Intelligence Community, the offensive cyber ***. *** source of Iranian offensive cyber activity ***. *** cyber-attacks on the petrochemical sector (which are explored in more detail below). GCHQ told the Committee ***:

> ***.[252]

334. As noted previously, it appears possible that there is a lack of effective co-operation in some areas of Iran's cyber and intelligence activity. The operational collaboration *** is a dangerous combination.

[251] Oral evidence – JIO, *** June 2023.

[252] Oral evidence – GCHQ, *** June 2023.

Actors: Iranian-aligned 'proxy' organisations

335. Non-state actors generally do not appear to have the capability to conduct significant offensive cyber-attacks. However, Lebanese Hizbollah and Hamas are more proficient and could be used as proxies to carry out such attacks. As noted previously, the cyber security industry has reported that Iran has provided Lebanese Hizbollah and Hamas with cyber assistance.

336. The Committee therefore questioned whether Lebanese Hizbollah – acting on behalf of Iran – posed an offensive cyber threat to the UK. GCHQ told us: "*** *there is potential for ... UK interest*[s] *to be caught up* ***".[253]

Targeted sectors

337. The threat of Iranian offensive cyber is particularly acute in the Middle East. However, NCSC has assessed that Iran has also used offensive cyber directly against the US, demonstrating its willingness to conduct cyber-attacks against Western nations if necessary, including the UK. NCSC judges that if Iran wished to conduct further offensive cyber activity against its adversaries such as the UK, it could include attacks against the petrochemical, utilities and finance sectors.

(i) Petrochemical

338. Since 2012, Iranian cyber actors have conducted a series of significant offensive cyber-attacks against petrochemical companies in the Middle East. The region's oil and gas industry is almost certainly a high-value target for Iranian cyber actors given its importance to the regional and global economy, with Middle Eastern countries representing five of the top ten oil producers worldwide and providing over a quarter of the world's global output.

339. The most significant examples of reported Iranian cyber-attacks in the petrochemical sector are known collectively as 'Shamoon' (1, 2 and 3), at least one of which is linked to ***. The attacks targeted various countries, predominantly in the Middle East but also further afield. The first attack, 'Shamoon 1', took place in 2012 and infected Saudi Aramco's systems (a Saudi oil and gas company and one of the largest companies in the world) and RasGas (a Qatari gas company). At the time, they were the most destructive cyber-attacks known to date, disrupting over 30,000 computers and forcing Saudi Aramco's corporate operations offline for five months.

340. In 2016, a second attack – known as 'Shamoon 2' – targeted a broad range of Saudi entities, forcing one chemical producer to shut down its operational processes temporarily. This included the destruction of ***.

341. In 2018, a third attack – 'Shamoon 3' – disrupted the operations of Italian *** oil and gas entities in the Middle East. It destroyed over 300 servers and 100 computers. Notably, whilst Shamoon 1 and 2 primarily affected Saudi entities, Shamoon 3 reportedly affected

[253] Oral evidence – GCHQ, *** June 2023.

servers in the UK, Italy and India, as well as those in the Middle East.[254] This was due to the interconnectedness of regional networks and global businesses and demonstrates how offensive cyber operations can cause significant unintended collateral damage.

342. Nonetheless, while the threat of collateral damage to the UK – such as its petrochemical sector – has increased with the growing interconnectedness of technology, NCSC's assessment remains that the UK is not the primary intended target for Iranian offensive cyber activity.

Offensive cyber-attacks – APT33

APT33 is an Iranian-linked cyber actor (***) and one of the most active cyber groups in the Middle East. It has undertaken both espionage and offensive cyber activity, which it is highly likely was in line with Iranian state strategic priorities, with a particular focus on Saudi Arabia and the Middle East's energy sector, targeting European and Middle East-based oil and gas companies. It has also targeted multiple other sectors, including government, finance, telecommunications, research, manufacturing and engineering.

It has also conducted 'spear-phishing' campaigns which are primarily focused on the Middle East and the US, and are likely to be a response to geopolitical tensions between the US and Iran.

Whilst the group has targeted the UK, it is highly likely that its UK targeting is a small fraction of its overall activity. NCSC assesses ***.

*** APT33 was almost certainly responsible for an offensive cyber-attack on the Middle East-based computer systems of a UK-headquartered oil services company. NCSC assessed that it was highly likely that the company had been targeted for its links to Saudi Aramco *** to degrade the Saudi petrochemicals sector rather than the company's connection to the UK. If this group is linked to the IIS *** this demonstrates Iran's willingness to risk collateral damage and the potential threat to UK energy security if Middle Eastern oil and gas companies are compromised.

343. Since the 'Shamoon' attacks, Iranian cyber actors have continued to pose a threat to the energy sector, conducting destructive cyber-attacks against Gulf petrochemical companies. Whilst Iran often does not state the motivations behind attacks, NCSC assesses that many of these attacks are likely to be in response to: cyber-attacks against Iran's oil and gas industry; the imposition of financial sanctions against Iran; and, more generally, heightened tensions due to geopolitical developments.

[254] 'Saipem Says Shamoon Variant Crippled Hundreds of Computers', Reuters, 12 December 2018.

(ii) Utilities/Critical National Infrastructure

344. Iran's intent to develop an offensive cyber capability to target CNI has historically been recognised by the Intelligence Community: *** Iran represents one of the highest threats to UK CNI, with cyber representing a key concern – albeit, as previously noted in this Report, Iran does not have the same sophisticated cyber capability as actors such as Russia and China: whilst in the current environment, Iran may not attempt an offensive cyber-attack specifically to damage the UK, collateral disruption is clearly a possibility.

345. Iran has continued to show concerning signs that both its intent and capability in this space are developing. In 2020, industry reporting indicated Iranian cyber actors targeted Israeli water facilities (but were ultimately unsuccessful), demonstrating an emerging capability against ICS. According to public reporting, Iranian cyber actors have also been linked to cyber security incidents affecting US CNI, including against power grid operators and a dam. The attack did no damage but they did reveal information about the computers running the operating systems, such as the flood control system.

346. In addition, in 2021 Iranian cyber actors attempted to disrupt services to patients at Boston Children's Hospital (***). This plot was subsequently disrupted ***. Iranian cyber actors also launched a series of attacks in 2022 against Albanian government infrastructure – it is likely that this was because Albania was hosting Iranian dissidents – which affected government services and resulted in the leaking of Albanian government data. This appears to be the first public reporting of Iran conducting a cyber-attack against the CNI of a NATO member.

Iranian attack on Israeli water facilities

In 2020, Iranian-linked cyber actors reportedly targeted at least two Israeli water facilities (***). This attack took place amidst heightened geopolitical tension between Israel and Iran, representing an example of Iran using asymmetric capabilities to respond to perceived aggression as a non-escalatory option.

None of the incidents reportedly caused damage or affected water supplies but Israeli officials believe that the intention of the attack was to manipulate the control systems into increasing the amount of chlorine in the treated water that is provided to Israeli homes. In a worst-case scenario, this would have led to hundreds of people becoming ill.

Fortunately, the attack was reported to have had a negligible effect. GCHQ noted to the Committee that it does not serve as evidence that Iran has the capability to damage CNI because it was ultimately unsuccessful.

Nonetheless, it appears to indicate an emerging Iranian capability and its deployment will presumably aid future development. It also highlights the potential life-threatening consequences of cyber-attacks on CNI.

347. We questioned the Intelligence Community about the potential threat to UK CNI and whether Iran had the level of sophistication to disrupt core CNI – switching off a piece of electrical generation equipment, for example – or whether disruption to supply chain businesses was more likely. GCHQ told us ***:

> **** have successfully caused disruption to business networks. ***.*[255]

348. The Committee questioned whether the ICS installed in Israel is similar to that used throughout CNI globally, including in the UK (if that were to be the case, the reported attack would indicate that, if Iran's intent and priorities towards the UK changed, it could use similar capabilities to target UK CNI). When we asked the Intelligence Community about this specific threat, GCHQ told us that ***:

> **** they have a degree of capability to interfere with Critical National Infrastructure services ... ***. We have seen it being deployed against others *** their capability to affect big business or the enterprise networks, so the usual, you know, office computers that we all use. ***.*[256]

349. Regardless of capability, as previously noted, it remains the case that in the current environment, Iran may not attempt to undertake offensive cyber activity specifically to damage the UK's CNI. ***. MI5 explained: "*they are not averse to it, they have no principled reason why they would not wish to do that, ****"[257]

(iii) Finance

350. Between 2012 and 2015, Iranian cyber actors conducted disruptive cyber activity against multiple institutions in the US financial sector. Whilst US organisations were the direct target, UK organisations were affected as collateral damage. Reporting states that the repeated co-ordinated attacks disabled bank websites and prevented customers from accessing their accounts, costing the financial institutions tens of millions of dollars. NCSC assessed that these attacks were in response to the imposition of financial sanctions on Iran and that the financial sector was likely to continue to be seen as a viable target for disruption, in response to further sanctions.

(iv) Other targets

351. Iran also has a history of conducting offensive cyber activity against other organisations and individuals, including opposition and dissident websites. This is highly likely to be intended to deter and discredit criticism of the Iranian government. Examples include the website of ***, which was *** to include adverse stories *** (and, ***, was caused by Iranian cyber hackers).

352. Separately, Iranian cyber actors have targeted private companies in the US. For example, in 2014 the US experienced its first known destructive cyber-attack when Iranian

[255] Oral evidence – GCHQ, *** June 2023.

[256] Oral evidence – GCHQ, *** June 2023.

[257] Oral evidence – MI5, *** June 2023.

cyber actors targeted the Las Vegas Sands casino, a company worth US$14 billion. The attack caused around US$40 million of damage, destroying three-quarters of the casino's servers, stealing information and defacing the website. The US Director of National Intelligence blamed the Iranian government for the attack when testifying before the Senate Armed Services Committee in 2015. According to NCSC, it is a realistic possibility that the motive for the attack could have been responding to anti-Iranian comments made by the casino's CEO, and this therefore appears to be a further example of Iran using cyber-attacks to respond to a perceived slight.

NN. Iran generally favours proportionality, responding in a similar way to perceived aggression. Where that is not achievable or realistic, it uses asymmetric capabilities – of which offensive cyber is a prime example.

OO. Offensive cyber – by which we mean both destructive and disruptive cyber-attacks – allows Iran to attack and contain Western and regional adversaries without resorting to conventional military action. It also provides Iran with a deniable tool with which to attack its enemies, respond to perceived aggression and project power in the region – and globally.

PP. Although Iran does not possess the same sophisticated cyber capability as Russia and China, it is an aggressive cyber actor, with a relatively high risk appetite. However, at present, it appears that the UK is not a top priority for Iranian offensive cyber activity and, in the current environment, Iran may not attempt an offensive cyber-attack specifically to damage the UK. Nevertheless, we note that this could change rapidly in response to regional or geopolitical developments: the likelihood has increased, for example, in connection with the recent protests in Iran.

QQ. Due to multinational trade and the interconnectedness of IT networks, it is likely that any global increase in Iranian offensive cyber activity increases the risk to UK entities – for example, through collateral damage resulting from broader activity. Iran both recognises and accepts that risk.

RR. If Iran decided to conduct an offensive cyber-attack against an adversary such as the UK, the petrochemical, utilities and finance sectors could be at risk. According to the National Cyber Security Centre, it is unlikely that all UK entities are able to detect or defend against Iranian offensive cyber activity.

SS. We were told that Iranian cyber actors *. *** they could *** attempt to cause *** disruption by targeting *** Critical National Infrastructure.**

TT. Whilst ultimately unsuccessful, we noted with particular concern that Iranian cyber actors reportedly targeted water facilities in Israel. When we questioned whether the Industrial Control Systems installed in Israel are similar to that used throughout Critical National Infrastructure globally, including in the UK, we concluded ***

THE THREAT: INTERFERENCE

What constitutes interference and influence?

As we noted in our *China* Report, the boundary between influence and interference is hard to define, but can be broadly articulated as the difference between those diplomatic and soft power activities that are generally considered 'legitimate', and those that are considered 'illegitimate' (although of course legitimacy is subjective and some countries are likely to set a lower threshold for which activities they consider to be interference in their affairs).

In 2020, the Joint State Threats Assessment Team (JSTAT) – after engagement with NSS and JIO – provided the following definitions for interference and influence activity (although this still does not reflect an agreed definition across HMG):[258]

> *Foreign influence is the capacity of power of foreign states or those acting on its behalf to be a compelling force on or produce effects on the actions, behaviour, opinions, etc. of others. In this case, we mean the combination of soft power (attraction) and hard power (coercion) by a nation state to achieve specific political, economic and security objectives. Influence operations are organised attempts to achieve a specific effect among a target audience by employing* [a] *diverse set of tactics, techniques, and procedures to affect the decision-making, beliefs, and opinions of a target audience. Influence activities include what would be commonly considered legitimate diplomatic activity and support for media organisations.*
>
> *Foreign interference comprises malign activity by a foreign state or those acting on its behalf which is designed to have or has a detrimental effect on the interests of the UK. This includes our government, democracy, public opinion, military, economy, critical infrastructure, academia, media, diplomacy, and UK-based diaspora communities. This activity can be deceptive, coercive or corruptive, and is not limited to the covert domain. It includes the use of agents of influence, leverage of investments, financial inducement, disinformation and cyber capabilities (disruptive/destructive/hack-and-leak).*

The Iranian interference threat to the UK

353. The Iranian regime believes that it is engaged in an active information conflict with its adversaries: both influence and interference activity are considered to be 'cognitive warfare capabilities'. The main purpose of this is opinion dominance. Whilst the UK will be a high priority target for Iranian interference activity, nevertheless it appears to be not as important as the US, Israel, Saudi Arabia or other Middle Eastern states. The importance of the UK is

[258] Written evidence – JSTAT, 2 November 2020.

probably due to its role in multilateral negotiations which touch on Iran's core interests, as well as the presence of several major Iranian-language news outlets in the UK, which are often critical of the regime.

354. It appears that Iran has historically posed a reasonable interference threat to the UK and its interests (which appears to be different in nature to the substantial interference threat explored in the Committee's previous Reports on *Russia* and *China*[259]). Given that the UK is a high priority target, it is possible that Iran's capability to undertake interference operations may be lower than its intent. The JIC Chair told the Committee: "***".[260]

355. The interference threat to the UK has recently been considered more significant; ***. This perhaps reflects the increase in the UK policy community's understanding, and also a wider consideration of the potential harm to the UK (for example freedom of speech) from Iranian interference activity, rather than a significant increase in Iranian interference activities against the UK. The Intelligence Community consider that Iran will almost certainly continue to use and develop interference activities around the world. It is possible that the increasing use of more complex interference operations by other nations such as Russia *** could influence Iran to develop its own methodologies. As noted above, it is possible that Iran's capability to undertake interference operations may be lower than its intent (***) and that the threat will increase slowly over time as Iran may seek to improve its capabilities. As a result, it is likely that the threat posed to the UK by such activity will increase; as with other types of Iranian threat, the extent of this increase will depend on the nature of the bilateral relationship between the UK and Iran.

356. Iran uses various actors and techniques, and its activities draw on the full range of state capability and are undertaken by the Iranian Intelligence Services (IIS), state media, Iranian-funded Islamic cultural centres and the Ministry of Foreign Affairs. The Islamic Revolutionary Guard Corps (IRGC) *** appears to conduct *** interference operations[261]. ***, all of which attempt to influence foreign elections, spread divisive narratives amongst Western populations and amplify narratives around IRGC operations. The Ministry of Intelligence and Security (MOIS) also appears to be involved in interference activity (particularly in the Middle East).[262] The Intelligence Community judged in *** that in the previous six months, Iran had attempted to manipulate *** to conduct interference activities on its behalf.

What is the effect of Iran's interference operations?

357. The effect of interference activity is very challenging to assess because it may be cumulative and long term, and the damage can vary greatly depending on the activity and the context in which it occurs. The assessment of this effect in the UK depends on the target. For

[259] *Russia*, HC 632, 21 July 2020; *China*, HC 1605, 13 July 2023.

[260] Oral evidence – JIO, *** June 2023.

[261] 'Iran Surges Cyber-enabled Influence Operations in Support of Hamas', Microsoft Threat Intelligence, 26 February 2024.

[262] 'Iran Surges Cyber-enabled Influence Operations in Support of Hamas', Microsoft Threat Intelligence, 26 February 2024.

example, some reports suggest that interference activities targeting dissidents in the UK have had a significant effect on their quality of life and ability to realise their rights to freedom of speech and association.[263]

358. Conversely, HMG considers that – overall – it is likely that Iranian interference operations have had a negligible effect on UK general public opinion and decision-makers. ***.

359. Director General MI5 explained ***.[264]

Who is Iran targeting and why?

360. Iranian interference activities against the UK are primarily conducted for one of four purposes, all of which are clearly linked to Iran's strategic objectives of maintaining the security of the regime, aspiring to be a regional power and containing the West:

- suppressing voices critical of the Iranian regime (targeting dissidents and other opponents of the regime);
- promoting views that align with Iranian geopolitical narratives (targeting the general UK population, including potential decision-makers);
- spreading narratives that undermine the British state and the UK–US alliance (targeting the general UK population, including potential decision-makers); and
- spreading the Iranian regime's religious ideology (targeting the Shi'a community).

(i) Suppressing voices critical of the Iranian regime

361. It is highly likely that Iran views the Iranian diaspora as the priority audience for its interference operations. The majority of this activity is focused on suppressing dissenting voices – such as those of dissidents, journalists and activists – in order to maintain the stability of the regime. The IIS are primarily responsible for this activity, and they often seek to achieve these goals through intimidation, thereby seeking to deter those in the diaspora from voicing criticism of the regime and undertaking anti-regime activities. Some reports suggest that this activity has a significant effect on the quality of life of those affected and the wider behaviour of the diaspora.[265]

(ii) Promoting Iranian geopolitical narratives

362. The National Cyber Security Centre (NCSC) assesses that Iran almost certainly seeks to influence international attitudes in line with Iranian strategic interests, enabled through *** influence operations. Cyber security industry reporting highlights that Iranian cyber

[263] '"We Live with a Gun to Our Heads": How Iran is Targeting Protesters in Britain', *The Guardian*, 18 December 2023; 'Iran is Targeting Its Opponents in Britain', *The Economist*, 8 February 2024.

[264] Oral evidence – MI5, *** June 2023.

[265] '"We Live with a Gun to Our Heads": How Iran is Targeting Protesters in Britain', *The Guardian*, 18 December 2023; 'Iran is Targeting Its Opponents in Britain', *The Economist*, 8 February 2024.

actors use a multitude of online personas to publish and push pro-Iran and anti-Western narratives (and that it is mainly spread *** through state broadcasting and public statements by Iranian politicians and the Supreme Leader).

363. Examples of the narratives spread by Western-facing, English-language Iranian sources include:

- criticism of the UK's support for Israel, UK arms exports to Saudi Arabia, and UK involvement in the Middle East;
- calls to remove US sanctions on Iran in response to Covid-19;
- the illegality of the US killing of General Qasem Soleimani, former Commander of IRGC Quds Force (IRGC-QF); and
- supporting the Iranian position on maritime disputes.

364. In light of this Committee's previous *China* Report, which found that decision-makers – including politicians, officials and the military – are key targets for Chinese interference operations (and the subsequent media reporting on alleged Chinese agents in Parliament), we wished to understand whether there is an equivalent Iranian threat. Iran appears to focus on influencing the UK population as a whole ***. The JIC Chair told us: "***";[266] however, MI5 noted that ***.

365. There are examples of Iran targeting the general population in order to influence political decision-makers indirectly on specific issues. For example, Iran uses the narrative that it is the UK Government's inflexibility that is preventing the release of UK nationals imprisoned in Iran as a particularly effective tool for generating public pressure, ***. Reuters reported on another example where politicians in the UK, Jordan, India and the Netherlands had all – presumably inadvertently – shared stories from covert Iranian news websites.

(iii) Spreading divisive narratives

366. Iran spreads divisive messaging to the UK public in an attempt to: undermine confidence in the British Government, its institutions and the UK press; undermine the UK–US relationship; and exacerbate wider social divides. Such divisive messages can be spread through overt and covert platforms and often focus on one side of a debate. Examples of divisive narratives spread by Western-facing, English-language Iranian sources include:

- criticism of the UK military or monarchy;
- accusation of UK support for terrorism;
- UK press bias or corruption in UK politics;
- poor morale in the Intelligence Community and intelligence failure;
- exacerbating UK–US tensions; and
- undermining UK attributions of hostile state activity.

[266] Oral evidence – JIO, *** June 2023.

Interfering in UK elections

367. Clearly the manipulation of elections represents one of the most damaging forms of interference and is an issue that this Committee examined in our previous *Russia* and *China* Reports. However, Iranian interference was not as apparent. ***[267]

368. Nevertheless, there is evidence which suggests that Iran had used social media to interfere with the democratic processes of the UK and other countries to:

- encourage a 'yes' vote in the 2014 Scottish Independence Referendum (via Iran-linked cyber actors);
- encourage ***; and
- attack ***.

369. As HMG explained:

> *There was some *** social media activity by the Iranians around the time of the Scottish independence referendum in 2014 ***. Nobody who has studied that activity believes it had any material influence of any sort. ****[268]

It appears that these efforts have had a minimal impact.

370. Our witnesses provided us with a broadly similar view of the prospects of Iran attempting to interfere in the next UK General Election. HMG told the Committee:

> *The track record of Iran on interference is ****[269]

Interference in Scottish Parliamentary Elections

In 2021, industry and media reporting stated that Iran probably attempted to influence the results of the Scottish Parliamentary Elections. Reporting stated that Iranian cyber actors targeted voters on Facebook and Twitter by creating false accounts, groups and pages, posing as Scottish people sympathetic to Scottish independence and encouraging real users to share pro-independence material – such as memes and cartoons – with their contacts online. As a result, Facebook reportedly removed hundreds of fake accounts and pages connected to Iran's state broadcaster during the first quarter of 2021.

Iran has a history of supporting particular narratives on this topic, including through PressTV, the Iranian state's primary English television channel, which routinely published content on Scottish independence throughout the Scottish election period.

The Intelligence Community told us that ***

[267] Oral evidence – ***, *** June 2023.

[268] Oral evidence – HMG, *** June 2023.

[269] Oral evidence – HMG, *** June 2023.

(iv) Spreading the Iranian regime's religious ideology

371. Iran targets Shi'a communities around the world to spread the teachings of the Supreme Leader and the political and religious ideology which underpins the Iranian regime. It follows that the Shi'a community in the UK is likely to be targeted as Iran views the UK – particularly London – as a global hub of Shi'a Islam.

372. Whilst the effect of Iranian interference activity on the Shi'a community is likely to be limited to those who are already sympathetic to the Iranian regime's religious doctrine, Iran uses a range of organisations in its efforts to achieve this influence, including:

- academic and student institutions;
- community, non-profit and youth organisations; and
- mosques and the Islamic Centre of England (ICE).

Methodology: intimidation

373. The IIS focuses their interference operations on harassment, making physical threats towards UK-based journalists and dissidents whom the Iranian regime perceives as undermining the security of the regime. These operations aim to intimidate the regime's perceived opponents and control the narrative being spread about the regime, reflecting the Iranian regime's core objective – survival. This activity includes sending threats to individuals via email and social media. The IIS also intimidate the friends and families of the Iranian diaspora who remain in Iran. MI5 explained this further:

> *The primary version of interference that we have seen over the last 18 months in the UK has been the concerted attempts to shut down dissidents or Farsi-language media organisations ... that has been by far and away the most prominent piece of attempted interference ...* ***.[270]

374. Aided by the Islamic Republic of Iran Broadcasting – the Iranian state media organisation (on which there is more detail below) – the IIS engage in public smear campaigns and broadcast forced confessions of dissident figures. Abductions and kidnappings are heavily publicised by state media to scare the diaspora, demonstrate the capability of the state to pursue dissidents beyond Iran's borders, and maximise the deterrent effect of these operations. Some reports suggest that this activity has had a significant impact on the behaviour of the Iranian community in the UK: targets of this intimidatory behaviour have limited their social contact with other Iranians, particularly those within Iran, moderated their criticism of Iran, and reduced their advocacy for contentious Iranian topics.

[270] Oral evidence – MI5, *** June 2023.

Targeting of an activist

According to an academic paper,[271] hours after an Iranian activist released a new book, a website was launched – by actors linked to the Iranian state – spreading disinformation about her, including allegations of immoral and financially corrupt practices. Multiple fake Facebook accounts circulated further rumours and allegations about her, including publicising her legal name, which she had not used for over two decades. Shortly after the website was set up, very similar content was released on Iranian state media, amplifying the covert messaging that had been spread on the internet and demonstrating the Iranian state's ability to co-ordinate the use of different platforms as part of its influence and interference operations.

375. In addition to individuals, the Iranian state targets organisations which it sees as critical of the regime. Examples include Iran International and BBC Persian. Family members of BBC Persian journalists in Iran have reported severe harassment, including being summoned for interrogations and threatened because their family members continue to work for the organisation. In June 2022, BBC Persian complained to the UN about the harassment its staff were receiving from the IIS. In October 2022, the Iranian Ministry of Foreign Affairs issued a statement naming BBC Persian in a list of individuals and organisations sanctioned for supporting terrorism, inciting violence, propagating hate speech and perpetrating human rights abuses.

Targeting of a Farsi-language media organisation – Iran International

The Iranian regime engaged in a campaign of intimidation against Iran International, a Farsi-language media organisation (probably due to the publication of anti-Iranian government narratives).[272] The IIS exerted pressure on family members of the organisation's journalists within Iran and threatened the journalists directly. Following Iran International's exposure of leaked audio recordings featuring the then Iranian Foreign Minister, Javid Zarif, ***.

In late 2022, there was a credible and imminent threat to the life of UK-based employees of Iran International. The media reported that a "*hostile Iranian surveillance team*" was allegedly seen outside journalists' homes and offices. *** In the following months, MI5 issued *** further 'threat to life' warnings to UK-linked individuals, some of whom were Iran International employees.

[271] 'State-aligned Trolling in Iran and the Double-edged Affordances of Instagram', Simin Kargar and Adrian Rauchfleisch, *New Media & Society* 21(7), January 2019.

[272] Iran International was originally based in the UK but temporarily relocated to the US in February 2023 following concerns about the security of its UK site (***). Following work by *** and *** to identify a suitably secure new site, Iran International returned to the UK in September 2023 and resumed producing news content in the UK.

In February 2023, Iran International decided to suspend its work in the UK temporarily and move to a more secure location. *** followed the arrest of an individual outside Iran International's headquarters after they were identified conducting suspicious activities. Iran International then ceased broadcasting news content from London and relocated to the US in response to the Iranian threat. HSG told the Committee that Iran International's decision to leave their previous location ***.[273]

The Committee asked whether the decision to relocate indicated that the US presented a harder operating environment for Iran than the UK – indeed, the Foreign Secretary told the Committee that the decision was "*unfortunate … It sends a negative signal*."[274] ***[275] ***[276]

376. The Committee is also aware of an Iranian soap opera which describes the British Embassy in Tehran as a "*nest of spies*" and uses real names of diplomats as characters – presumably in an attempt to try and create an intimidatory atmosphere towards UK nationals in Iran.[277]

Methodology: hack-and-leak

377. Whilst Iran almost certainly possesses the capability to conduct a 'hack-and-leak' operation against governments, political parties and public figures, ***, there have been examples of such operations in the Middle East. For example, in 2021 a house cleaner for Israel's Defence Minister was arrested for engaging with an Iranian cyber actor – named in media reporting as the 'Black Shadow' group – and offering to plant a bug on the Defence Minister's computer. It is almost certain that the cyber actor would be willing to leak the information obtained, particularly as it has previously leaked identifiable information belonging to Israeli military personnel and citizens.

378. Since 2020, there has been an observed increase in Iranian hack-and-leak activity. Iranian cyber actors are highly likely to have acquired material from their espionage activities in the UK which could be used to cause reputational damage if released. Whilst Iran may not use a hack-and-leak operation to interfere directly in a UK General Election ***.

Saudi Foreign Ministry – Iranian 'hack-and-leak' operation involving UK information

In 2015, Iranian cyber actors compromised the Saudi Arabian Ministry of Foreign Affairs, following which Wikileaks obtained a large number of related documents. As was publicly reported in the media,[278] the leaked material included confidential information relating to the UK–Saudi relationship, which was the subject of international media and UK Parliamentary attention.

[273] Oral evidence – HSG, 21 June 2023.
[274] Oral evidence – Foreign Secretary, 6 July 2023.
[275] Oral evidence – MI5, *** June 2023.
[276] Oral evidence – MI5, *** June 2023.
[277] Oral evidence – ***, *** June 2023.
[278] 'UK and Saudi Arabia "in Secret Deal" over Human Rights Council Place', *The Guardian*, 29 September 2015.

Methodology: traditional and social media

'Independent' news websites

379. The Iranian regime routinely uses websites and social media as platforms for interference, including networks of purportedly 'independent' news websites. This activity includes using fake media companies, obfuscated press releases and purportedly non-Iranian news websites. The number of such websites is significant. For example, in 2018 cyber security companies Clearsky and FireEye identified almost 100 fake media outlets operated by Iran, each with their "*own websites, social media accounts, and pages that distribute 'fake news' worldwide*". These websites operate across 28 languages (with the two most common languages being Arabic and English).[279]

380. The disinformation that they publish varies depending on the country being targeted and its relationship with Iran. The websites use different methods, including: copying and stealing sympathetic content from legitimate media outlets; stealing and editing articles to better fit the intended narrative; and creating bespoke content. In order to strengthen the credibility of the websites, irrelevant content (i.e. unrelated to the Iranian regime's cause) is often uploaded.

381. Intelligence has linked some of these websites to ***, which has at least ***. *** write and commission articles for publication on a network of news websites with no stated link to Iran ***. Intelligence also indicates that *** is able to pass information to mainstream news networks whilst obfuscating its origin.

382. In June 2021, the US Department of Justice seized 33 websites, both overtly and covertly linked to the Iranian state. These included three websites operated by Kata'ib Hizbollah, an Iranian-aligned militant organisation based in Iraq. Whilst this disruption almost certainly reduced Iran's capabilities to disseminate its narratives online in the following months, ***.

Social media

383. Social media represents a relatively cheap, flexible and effective method for Iran to undertake influence and interference activity. Social media now plays a central role in how individuals access news and information and social media accounts are relatively easy to create and maintain when existing accounts are disrupted, unlike traditional media (a particular concern for Iran which has suffered economically following the implementation of international sanctions). The Iranian regime has set up a vast number of social media accounts to support its networks of fake websites. These include accounts that purport to belong to real people from the target country, which propagate the website's articles via their feed, maintaining large networks of contacts.

[279] 'Global Iranian Disinformation Operation', Clearsky Cyber Security, November 2018.

Suspension of Twitter accounts linked to Iranian cyber actor

Prior to September 2020, Twitter suspended a large number of accounts operating from Iran.[280] These accounts pretended to be from the West or the Middle East, and sometimes posed as journalists. The topics of tweets included Black Lives Matter and Covid-19, as well as innocuous content which was published in order to make the fake accounts appear more credible. ***.

Television and radio

384. The IRIB (Islamic Republic of Iran Broadcasting) media corporation operates international, national and provincial services and is responsible for influence activity on behalf of the Iranian state. It has an annual budget of over US$1 billion and has branches in 20 countries worldwide, including the UK. Its head is appointed directly by the Supreme Leader and several heads used to work for the IRGC. Its coverage includes over 50 channels, 18 of which are available to view in the UK. It also operates a world service radio station, which is broadcast in 32 languages. According to research conducted by the School of Oriental and African Studies at the University of London, the Iranian diaspora in the UK watches IRIB channels more than any other media but this is mainly entertainment content rather than news. In relation to covert social media activity, in April 2020 Facebook took down 500 pages, groups and accounts that were linked to fake 'independent' news websites attributed to the IRIB.

PressTV – Iran's primary English channel

IRIB's primary English-language channel is PressTV, which was set up in 2007 and has an annual budget of c.US$25 million. At the time of its establishment, the Iranian government stated that it intended to use it to counter what Iran perceived as Western propaganda. In 2010, PressTV was fined £100,000 for broadcasting an interview with a documentary maker that had been obtained under duress. Its licence was revoked by Ofcom in 2012 and it was removed from air for breaching broadcasting licensing rules in the UK.

However, PressTV maintains an extensive social media presence and its website is still accessible within the UK (which like other overtly Iranian state-linked websites has been set up on Iran-based servers outside of US jurisdiction). It has dedicated platforms on Facebook, Twitter and YouTube (although its channel was deleted by YouTube in 2020, and repeated removal of its accounts by social media platforms continue to cause disruption). A significant minority of PressTV content is disinformation, with the majority being factual but with a heavy editorial slant.

[280] ***

385. Despite the significant number of Iranian state-affiliated websites, social media platforms and television channels, they have relatively low levels of UK audience engagement compared to mainstream news sources and equivalent Russian platforms.

Methodology: Iranian organisations in the UK

The Iranian Embassy in the UK

386. Similar to other embassies around the world, the Iranian Embassy in the UK plays a role in attempting to shape the UK public perception of the country and influence bilateral issues. A previous Iranian Ambassador to the UK, Hamid Baeidinejad (2016–2021) frequently used Instagram and Twitter to propagate views that aligned with Iran's geopolitical narratives. Activity such as this is entirely legitimate. However, some activity strays into interference when, for example, Ambassador Baeidinejad consistently sought to undermine the credibility of UK-based Farsi-language channels such as BBC Persian and Iran International, forming part of the wider campaign of Iranian state activity targeting opponents of the regime. In 2019, Reporters Without Borders – a charity which safeguards the right to freedom of information and defends independent journalism – criticised the Ambassador for threatening Iranian journalists abroad, particularly those in the UK.

Iranian cultural and religious organisations

387. During this Inquiry, we have sought to establish whether the Islamic and cultural institutions that Iran supports and funds in the UK pose a threat. Whilst these provide legitimate support networks for the Shi'a community, they are also likely to be used to promote the ideology of the Supreme Leader. Nevertheless, many people within the Iranian diaspora would feel uncomfortable attending events organised by the Iranian state and it is highly likely that Iranian state-backed cultural organisations currently have minimal influence over the opinions and actions of the Iranian diaspora. The links between Iran and these organisations are often deliberately concealed to increase their credibility and purported neutrality. This even includes entities connected to ICE, Iran's principal official religious institution in the UK. For example, the Manchester branch of ICE's website includes no obvious reference to the Supreme Leader, obscuring this connection, possibly in an attempt to appeal to Manchester's student population.

388. Professor Ansari emphasised the threat of clerics who deliver talks at venues such as ICE, stating:

> *The Imams who are sent are financed by the* [Iranian] *state. They are here on* [its] *behalf, not on behalf of Shi'a Muslims in Britain ... and they have a direct link therefore to the* [Iranian] *state ... that is something that I think we need to take much more seriously in the current climate.*[281]

[281] Oral evidence – Professor Ali Ansari, 23 March 2023.

Professor Ansari also noted that, following the attack on Sir Salman Rushdie in 2022:[282]

> *the head of the Islamic Centre at Maida Vale made some sort of great celebration about how marvellous this was ... given that he was a charity in receipt of furlough ... I thought it was pretty shocking. It is extraordinary. Now, why isn't action being taken? If action is not being taken, where is the deterrent?... He just carries on. He will carry on and he will continue using British taxpayers' money to do it.*[283]

389. When we asked the Home Secretary about the potential threat posed by ICE and other such organisations, she told the Committee that there is evidence indicating that ICE is highly likely to be operating with the approval of the Iranian regime and working with other educational institutions to promote extremist ideology. She explained that this included:

> *incendiary language used against protesters in September 2022. There are reports ... of the ICE intimidating protesters ... And it is highly likely that institutions, educational institutions linked with the ICE, including the Irshad Trust, the Islamic College of Advanced Studies and Hawza Ilmiyya also promote 'Khomenei-ism', and that is due to multiple links between these organisations through a crossover of staff and speakers, as well as previous trustees and family members. So there is a whole ecology of these organisations operating, promoting extremist ideology, promoting violence and inciting hatred.*[284]

390. We have previously reported in the 'Espionage' chapter that ***. In this context we also note HSG's reporting that *** is around the "*malign influence of regime linked groups … in particular here I would point to the cultural centres, so ICE, for example*".[285]

391. We have also noted media reports in 2023 that the IRGC had allegedly attempted to radicalise British university students through online talks hosted by the Islamic Students Association of Britain (ISA). The IRGC officers reportedly espoused anti-Semitic and violent views, urging students to support illegal attacks and venerating people who had carried out acts of aggression. Whilst the ISA denied any affiliation with the IRGC, the media reported that its former chair had recently been granted an audience with the Iranian Supreme Leader.

392. This appears to be the first indication of the IIS attempting to directly engage with, and influence, students in the UK. When we questioned the Intelligence Community on the specific threat of this engagement, we were surprised by the lack of detail with which we were provided, which linked the threat to a broad range of – mostly unrelated – hostile activity against academia. In doing so, it appeared to play down the concern of the IIS directly engaging with students in the UK:

[282] In 1989, the then Supreme Leader of Iran, Ayatollah Khomeini, issued a fatwa ordering Muslims to kill Salman Rushdie in retaliation for his authorship of *The Satanic Verses*. Rushdie was attacked and seriously injured in 2022, potentially in connection with this fatwa.

[283] Oral evidence – Professor Ali Ansari, 23 March 2023.

[284] Oral evidence – Home Secretary, 6 July 2023.

[285] Oral evidence – HSG, 21 June 2023.

> *the IIS may look to target students and wider academia ... to fulfil a broad range of objectives, such as transnational repression and monitoring of dissidents and critics of the Iranian regime; information acquisition, to provide Iran with a strategic advantage; or the recruitment of students for long-term seeding operations.*[286]

UU. The Iranian regime believes it is engaged in an active information conflict with its adversaries and refers to interference activity as 'cognitive warfare'.

VV. Iran draws on the full range of state capability to conduct interference operations. This includes the Iranian Intelligence Services, state media, the Iranian Ministry of Foreign Affairs and Iranian-funded organisations. They use different platforms – both overt and covert – such as traditional media, social media and networks of purportedly 'independent' news websites, to spread their own narratives in the UK.

WW. Whilst the UK is a high priority target for Iranian interference activity due to its role in multilateral negotiations relating to Iran and the presence of several Iranian-language news outlets in the UK which are critical of the regime, it is not as important as the US, Israel, Saudi Arabia or other Middle Eastern states.

XX. Overall, HMG considers that Iran's interference operations (which seek to suppress critical voices, promote views that align with its own geopolitical narratives and religious ideology, weaken confidence in British institutions, undermine the US–UK relationship, and exacerbate wider social divides) have had a negligible effect on UK public opinion and decision-makers, including in relation to UK elections.

YY. The focus of Iran's interference operations – and of most concern – are the attempts to intimidate Iranian dissidents and those working for media organisations such as Iran International in the UK and beyond. Some reports suggest Iran's efforts to intimidate the regime's perceived opponents have had a significant impact on the Iranian diaspora community in the UK: targets of this intimidatory behaviour have limited their social contact with other Iranians, particularly those within Iran, moderated their criticism of Iran, and reduced their advocacy for contentious Iranian topics. We note and encourage ongoing efforts to support Iran International's return to the UK. However, we are concerned as to whether this means the UK is not a sufficiently hard operating environment for Iran, and whether HMG is taking sufficient proactive action to protect UK-based media organisations.

ZZ. Whilst the Islamic Centre of England and other cultural and educational centres supported by Iran have legitimate roles supporting the Iranian diaspora, there are grounds to suggest that they have been used to promote violent and extremist ideology. This threat must not be underestimated.

[286] Written evidence – HMG, 31 August 2023.

THE THREAT: TO UK INTERESTS IN THE MIDDLE EAST

393. The UK has substantial security and commercial interests in the Middle East, which are at risk from Iranian hostile activity. The UK's security interests include the need to protect dual nationals in the region, Embassy staff, and our Armed Forces. The UK's commercial interests in the region include extensive trade and investment, as well as energy security – indeed, the UK's reliance on gas and oil exports from the Middle East is increasingly significant in the context of Russia's invasion of Ukraine in February 2022.

394. There is a broader risk to UK interests writ large if there is increased instability in the region. Increased instability in the Middle East – from Iran or otherwise – represents a security threat to UK nationals and Armed Forces stationed in the region, and also – given the consequent increase in migration, the international reach of terrorism and the risk of increased proliferation – to those living in the UK. Disorder in the Middle East is likely to increase the space for terrorist and extremist groups to operate (as noted in the Government's 2021 Integrated Review). We note the observation of the Select Committee on International Relations in 2017, "*what happens in the Middle East does not stay in the Middle East*".[287]

395. In 2014, despite being home to just 5% of the world's population, the Middle East accounted for 45% of the world's terrorist attacks, almost 70% of battle-related deaths and almost 60% of global refugees.[288]

Overarching threat in the region

396. There are a number of aspects of the threat to UK interests in the Middle East, including:

- a physical threat to UK nationals in Iran (and the wider Middle East);
- a threat to UK maritime and commercial interests in the region, including access to energy; and
- a security threat in respect of terrorism, increased migration and nuclear proliferation.

397. The Committee was told that the level of physical threat posed by Iran to UK nationals in the region had increased in recent years and is now significant (***). As with the increased threat to UK-based individuals and organisations which Iran perceives as a threat to the regime (connected to the recent protests in Iran), this shows the Iranian regime's concern about internal security and suggests a demonstrable link between the threat posed by Iran and its main objective of protecting the regime.

398. In terms of threatening UK interests in the region, Iran has a broad range of tools that it could deploy if it deemed it necessary. These include: missiles and drones which it could use against Israel, regional US bases (where UK forces are co-located) and Gulf energy infrastructure (e.g. oil supply); its network of aligned militant and terrorist forces; offensive

[287] 'The Middle East, Time for New Realism', Select Committee on International Relations, 2 May 2017.
[288] 'The Middle East, Time for New Realism', Select Committee on International Relations, 2 May 2017.

cyber; the ability to disrupt shipping in the Gulf; and chemical weapon capabilities.[289] The Chief of Defence Intelligence (CDI) summarised that: Iran poses an aggressive threat to the "*safety of British nationals, tourists or expats … deployed forces in the region …* [and] *trade through the Straits of Hormuz*".[290] Nevertheless, it would appear that overall Iran's capability is higher than its intent.

Threat to individuals

(i) Detention of dual nationals

399. Despite the small number of Western visitors and the lack of Western economic interests in Iran, arbitrary arrest and detention remains the primary physical threat to British nationals in Iran. As Foreign, Commonwealth and Development Office (FCDO) travel advice on Iran acknowledges, British nationals "*could be arbitrarily arrested, questioned or detained*".[291] This risk is heightened in relation to British-Iranian dual nationals. Professor Ansari told us: "*the greatest, and most obvious threat ... is* [to] *dual nationals ... what is happening in terms of hostage-taking*".[292]

400. The risk of arbitrary detention for Iranian dual nationals is exacerbated as dual nationality is not recognised by Iran. This means that the Iranian government will not grant consular access to foreign officials to visit dual Iranian nationals in detention. Even in the case of mono-UK nationals, the Iranian authorities can be slow in allowing a consular welfare visit and have in the past failed to meet their international obligations to notify embassies when foreign nationals have been detained. Many international institutions have criticised the Iranian regime for this practice. For example, Human Rights Watch cautioned that "*politically motivated arrests*" of dual and foreign nationals in Iran had increased, particularly those whom Iran perceives to have links with Western academic, economic and cultural institutions, often accusing them of espionage.[293]

401. Of the publicly reported 66 cases of detained foreign and dual nationals in Iran between January 2010 and November 2021, academic research found that nationals of the US, UK, Canada and France were over-represented. The US accounted for 20 and the UK accounted for 14.[294] The US government has described the Iranian use of arbitrary detention of US nationals as "*hostage-taking*", and in April 2023 the US Department of the Treasury sanctioned four Islamic Revolutionary Guard Corps Intelligence Organisation (IRGC-IO) senior officials for their role in the "*hostage-taking or wrongful detention of US nationals in Iran*".[295]

[289] With regard to chemical weapon capabilities, the US Intelligence Community assessed in 2024 that "*Iran probably aims to continue research and development of chemical and biological agents for offensive purposes. Iranian military scientists have researched chemicals, toxins and bioregulators, all of which have a wide range of sedation, dissociation, and amnesiac incapacitating effects*." (Annual Threat Assessment of the US Intelligence Community, 5 February 2024.)

[290] Oral evidence – DI, *** June 2023.

[291] 'Iran, HMG Travel Advice', GOV.UK, accessed 20 January 2023.

[292] Oral evidence – Professor Ali Ansari, 23 March 2023.

[293] 'Dual Nationals Imprisoned in Iran', House of Commons Library, 17 January 2023.

[294] 'Iran's Arbitrary Detention of Foreign and Dual Nationals as Hostage-taking Crimes Against Humanity', *Journal of International Criminal Justice*, 7 March 2022.

[295] 'Treasury Sanctions Officials of Iranian Intelligence Agency Responsible for Detention of US Nationals in Iran', US Department of the Treasury, 27 April 2023.

402. Iran may arbitrarily detain dual nationals for several reasons – perhaps due to genuinely held suspicions within the Iranian security apparatus, or for use as political leverage on areas of strategic interest and/or as pawns in internal rivalries within the regime. However, it is also possible that there may not be a consistent view about dual nationals within the Iranian regime.

403. The threat of arbitrary detention has increased since the recent protests in Iran, once again demonstrating how internal (in)stability within Iran affects the threat to UK nationals. The Iranian judiciary has announced that 40 foreign nationals have been detained since the protests began due to their suspected involvement in the protests, of whom several may be British[296] nationals (at the time of writing, this was unconfirmed).

Detention of Nazanin Zaghari-Ratcliffe

Nazanin Zaghari-Ratcliffe is a British-Iranian dual national. In 2016, she was detained whilst visiting her parents in Tehran. She worked for the Thomas Reuters Foundation, which aims to advance media freedoms and promote human rights. She was arrested in Iran on charges of espionage and leading a foreign-linked hostile network.

She was sentenced to five years in prison and subsequently sentenced to a further year in 2021 for alleged propaganda against the Iranian government. Many – including Zaghari-Ratcliffe's MP, Tulip Siddiq MP – have suggested that her detention was linked to the UK's historical International Military Services (IMS) debt owed to Iran,[297] although this was denied by successive British Prime Ministers who lobbied for Zaghari-Ratcliffe's release.

***

Zaghari-Ratcliffe was released in March 2022 at the same time as the UK paid the IMS tank debt to Iran (which the then Foreign Secretary said was ring-fenced so that Iran could only use it for the purchase of humanitarian goods). The Prime Minister's spokesman stated that the payment was "*not contingent on the release of any detainees*", and that HMG had "*never accepted our nationals being used as political leverage, including to settle the IMS debt repayment*".[298] ***.

(ii) Attacks on the British Embassy and its staff in Tehran

404. Whilst it appears relatively unlikely, the British Embassy in Tehran is a potential target for an attack (and locally engaged staff may be at increased risk). ***.

405. The relative likelihood of these threats will clearly be driven by a combination of political, social and economic factors. One of the most significant factors is the nature of the

[296] ***

[297] For more detail on the IMS debt, see the box on 'UK–Iran relations' on page 29.

[298] 'Nazanin Zaghari-Ratcliffe and Anoosheh Ashoori Back with Families', BBC News, 17 March 2022.

bilateral relationship between Iran and the UK (for example, negotiations around a nuclear deal). Any significant decline in the bilateral relationship will presumably lead to an increase in the physical threat to Embassy staff. ***.

406. Other factors that could increase pressure on the Embassy in Tehran may include:

- The election/appointment of a greater number of conservative 'hard-liners' within the Iranian regime, who are more averse to engagement with the West.
- ***.
- A reduction in general regime cohesion.
- General anti-UK sentiment.
- Social unrest, ***.

Conversely, it appears that a desire on Iran's part to be seen as a responsible state actor, to maintain a dialogue with the UK and to avoid an unmanaged escalation in tension, may all contribute to reducing the pressure on the British Embassy.

407. Different elements of the Iranian regime may have different thresholds for targeting the Embassy, *** For example, Iran's national police detained the UK Ambassador in 2020, accusing him of participating in anti-regime protests (which appears to have been aimed at directing public anger towards perceived British interference). The Iranian Ministry of Foreign Affairs quickly intervened to secure his release, with media reports suggesting this indicated disagreement within the regime. ***.

408. The UK diplomatic presence in Iran represents a 'Western' target, vulnerable to political and societal anti-Western sentiments. There is a risk that protests, anti-British rhetoric and anger towards the UK presence could inspire individuals to target British Embassy staff. For example, in 2019 a vehicle intentionally crashed into the gates of the Embassy compound (but no attempt was made to enter the site). The Chief of SIS noted that: "*in relatively recent memory, our Ambassador has been detained ***. So, given those behaviours, one is always very, very aware of the risks that our diplomatic personnel run in Tehran and that is kept under ... extraordinarily careful review by the Foreign Office*."[299] The JIC Chair told the Committee:

> *we are always conscious that there is a threat, a potential threat ... to the Embassy in Iran. There is no American Embassy, there is no Israeli Embassy and therefore, if Iran faces a sea of troubles, then the United Kingdom ... may very often be the epicentre of protest.*[300]

We consider that the recent protests in Iran following the death of Mahsa Amini in Iranian police custody have increased the pressure on the British Embassy, including of intimidation and harassment.

[299] Oral evidence – SIS, *** June 2023.

[300] Oral evidence – JIO, *** June 2023.

Attack on the British Embassy in Tehran in 2011

In 2011 the British Embassy in Tehran was attacked by a mob who ransacked offices, burned British flags and briefly detained staff. It was publicly reported that Iranian security forces did not stop the protesters as they forced their way into the Embassy.

It was also reported that the attack was a response to sanctions that had been imposed by the UK on Iran in relation to its nuclear programme and took place a day after Iran's Parliament approved a measure to expel the UK Ambassador and downgrade diplomatic relations between Iran and the UK.

The media suggested that the attack reflected factionalism within the regime, with the Iranian Foreign Ministry expressing regret for the attack. The Iranian authorities are believed to have been connected to the attack, reflecting sustained pressure on the Embassy.

In response, the UK closed the Iranian Embassy in London (and its own Embassy in Tehran), suggesting that the attack could not have taken place without the approval of the authorities. The UK restored the Embassy in 2015 following the signing of the Joint Comprehensive Plan of Action (JCPOA) nuclear deal.

409. As above, at the time of taking evidence for this Inquiry, an Iranian attack against the British Embassy in Tehran appears relatively unlikely. ***[301] ***[302]

(iii) Collateral damage from tensions in the region

410. We have previously covered the network of militant and terrorist groups across the Middle East which Iran supports (in the 'Iran's International Partnerships' chapter). These groups pose a threat to UK interests in the Middle East, whether following direction from Iran or – particularly in the case of the military – as collateral damage. This threat of collateral damage (resulting from misidentification or miscalculation) is the main physical risk to British nationals in the Middle East (outside of Iran), due to the sizeable number of UK Armed Forces in the region and their co-location with more heavily targeted US forces. For example, a rocket attack on the Camp Taji military base in Iraq in March 2020 led to the death of a British servicewoman (and two Americans) and injuries to many others. According to the US, this attack was conducted by Kata'ib Hizbollah, an Iraqi Shi'a militant group which receives significant support from Iran.

[301] Oral evidence – ***, *** June 2023.

[302] Oral evidence – ***, *** June 2023.

(iv) A ballistic missile attack

411. One of Iran's key asymmetric capabilities which – together with its regional network of aligned militant and terrorist organisations – help it to deter adversaries is its extensive ballistic missile programme. It has a large number of short- and medium-range systems which enable it to threaten UK interests – such as deployed forces – throughout the Middle East.

412. Since 2010, there has been a significant improvement in Iran's missile range, accuracy and effectiveness. ***. Iran has also attempted multiple satellite launches, demonstrating the development of longer-range missile technology. It has the capability, either directly or through its partners, to strike UK military bases overseas. For example, the ballistic missiles it has provided to Lebanese Hizbollah could strike UK Armed Forces ***.

413. This missile capability has been used to target the UK's regional allies ***. In 2019, Iran almost certainly used missiles and drones to target Saudi Arabia's oil infrastructure, in response to the US policy of 'maximum pressure'. In addition, in 2020 Iran launched a ballistic missile strike against Coalition forces at the Ayn al-Asad airbase in Iraq in response to the US killing of IRGC Quds Force (IRGC-QF) Commander General Qasem Soleimani.

(v) A Chemical and Biological Weapons attack

414. As noted earlier, the US Intelligence Community assessed in 2024 that Iran probably sought to develop its Chemical and Biological Weapons (CBW) capabilities. The overall CBW threat to UK forces on counter-insurgency and stabilisation operations will probably therefore increase over the coming years. ***. UK forces deployed in the region are therefore probably at risk from CBW – i.e. in the event of a direct conflict with Iran, UK forces could face a CBW attack.

415. When we questioned the Intelligence Community on the CBW threat from Iran, SIS told the Committee that ***.[303] This appeared to contradict what the JIC Chair told us subsequently, that "***".[304] However, the Intelligence Community subsequently clarified that ***. (We also note that, as will be explored in the Response section of this Report, ***.)

416. CDI told the Committee that it is worth noting that: "*as a general assessment point, we assess that* ***" – although DI later noted that it was nonetheless highly likely that ***

The threat to UK maritime, commercial, energy and security interests

417. Iran possesses several capabilities that could be used to inflict significant economic harm to UK interests in the Middle East – *** there *** appears to be a reasonable threat of sabotage and economic disruption ***. As previously noted, historically Iran has not appeared intent on using these capabilities to their fullest extent.

[303] Written evidence – HMG, 21 April 2022.

[304] Oral evidence – JIO, *** June 2023.

418. The threats to UK interests in the region include:

(i) Physical (or cyber) attacks on oil or gas or other UK economic interests in the Middle East.

(ii) Disruption to shipping through the closure of key routes.

(iii) Attacks on, or seizures of, shipping.[305]

(i) Physical (or cyber) attacks on oil, gas or other UK economic interests in the Middle East

419. The threat of collateral damage to UK interests in the region from Iranian offensive cyber activity has already been explored in the 'Offensive Cyber' chapter. This section therefore focuses on the threat of a physical attack.

420. Iranian-supported unmanned aerial vehicle (UAV) attacks on Saudi infrastructure are not uncommon and have previously been claimed by and attributed to the Houthi militant group in Yemen (which is militarily supported by Iran). However, other Iranian-supported militant groups are also likely to have targeted oil interests in the Middle East. For example, in mid-2019, explosive UAVs damaged two oil pumping stations in Saudi Arabia ***.

421. International media outlets have reported on many of these attacks. In September 2019, two critical Saudi oil facilities were attacked, representing the single largest daily oil supply disruption in history. The total supply loss from these facilities being taken offline amounted to approximately 5.7 million barrels of oil per day, representing more than half of Saudi Arabia's total output and over 5% of the global supply, causing oil prices to soar. A joint statement issued by the heads of the UK, France and Germany said that "*it is clear to us that Iran bears responsibility for this attack. There is no other plausible explanation*", and the US was reported in the media to have identified that the drones and missiles had been launched from Iran.[306]

(ii) Disruption to shipping

422. Iran is one of the few countries that has threatened freedom of navigation for UK commercial shipping, primarily in the Strait of Hormuz. The Strait of Hormuz is a critical strategic channel controlled by Iran through which around 30% of the world's seaborne-traded crude oil passes every day. However, whilst Iran regularly practises its capability to close the Strait – which would significantly disrupt oil supplies from the Gulf – it would be a major step for Iran to do so.

[305] We have noted previously that attacks on commercial shipping conducted by the Houthis from November 2023 took place after our evidence-taking concluded.

[306] 'Joint Statement by the Heads of State and Government of France, Germany and the United Kingdom', 23 September 2019.

(iii) Shipping attacks and seizures

423. Iran is able to take advantage of the constrained entry point to the Strait, which allows it to deploy boats quickly – if necessary – to interfere with naval and merchant traffic. Iranian naval forces – including the regular Iranian Navy and the IRGC Navy – have a range of capabilities that can be used to threaten maritime interests in the region, including anti-ship and coastal cruise missiles, naval Special Forces, sea mines, explosive boats, fast-attack craft, UAVs and small submarines.

424. Whilst Iran has the capability to harass, board, seize, attack or sink any merchant vessels – including those belonging to the UK – operating in the Gulf, Strait of Hormuz or Gulf of Oman, Iran may not choose to do so unless responding to a perceived act of aggression. As DI told us:

> *Iran almost certainly seizes tankers to retaliate against international sanctions enforcement ... and to deter future action against the oil trade* [and also as a] ... *reciprocal response, at least in terms of their perception ...* [regarding] *action taken against them.*[307]

425. The Iranian maritime threat increased following the US withdrawal from the JCPOA nuclear deal in 2018 and the US reimposition of sanctions on Iran. This escalation in tensions led to a greater number of Iranian-supported attacks on Saudi oil infrastructure and more frequent Iranian interference with merchant shipping in the Gulf. The JIC Chair explained that "*this was clearly an attempt by Iran to exert leverage on the nuclear negotiations*".[308]

Seizure of the Stena Impero

In July 2019, the *Grace One*, an Iranian-flagged ship, was seized by British Royal Marines and Gibraltarian authorities for carrying Iranian crude oil to Syria in breach of EU sanctions. The Iranian regime described the seizure as illegal. It is clear that the threat from Iran to the UK increased as a result – at least in the short term (***). A British-flagged vessel – the *Stena Impero* – was indeed targeted later that month, causing a further escalation in tensions and demonstrating Iran's ability to disrupt commercial traffic and target UK interests directly. Since the UK's seizure of *Grace One*, Iran is likely to perceive the UK to be more closely aligned with the US campaign of 'maximum pressure', which – as a consequence – may have increased the Iranian threat posed to UK interests in the region.

426. However, since then the maritime threat has clearly reduced. The JIC Chair suggested that "**** that* [strategy] *just had not worked very well and therefore we are seeing a lot less of it*" (although we note that ***). Disruption of commercial shipping (such as harassment, attacks and seizures) also has the potential to anger a wide range of countries – including China – which currently purchases a significant amount of oil from Iran.

[307] Oral evidence – DI, *** June 2023.

[308] Oral evidence – JIO, *** June 2023.

427. Nevertheless, it appears that Royal Navy units operating in the Persian Gulf and the Strait of Hormuz will continue to encounter both the IRGC Navy and Iranian Navy. Whilst there is a realistic possibility that there will be incidents that breach maritime customs and threaten safety, DI assesses that there is only a remote chance that such engagement would lead to a direct threat to UK forces (unless there was a further worsening of tensions between the UK and Iran). However, even if there is no Iranian intent to target UK maritime interests directly, there is a realistic possibility that UK interests will be affected as collateral damage – this was demonstrated in 2021 by the attack on the Israeli-linked *MV Mercer Street* in the Gulf of Oman.

Attack on MV Mercer Street

In July 2021, *MV Mercer Street*, a maritime vessel owned by an Israeli company listed in the UK, was attacked in the Gulf of Oman (reflecting the higher threat posed to Israeli-linked vessels). This followed a series of 'tit-for-tat' attacks between Israel and Iran. The Intelligence Community assessed that Iran attacked the vessel in international waters near Oman, using one or more UAVs. The attack resulted in the death of a UK national and a Romanian national. Whilst Iran almost certainly did not conduct the attack with the intention of killing a UK national, it demonstrates the risk of UK interests being unintentionally affected as collateral damage, particularly as a result of heightened tensions between Iran and Israel.

Impact of the killing of General Soleimani

428. In January 2020, the US killed IRGC-QF Commander General Qasem Soleimani. This led to a significant increase in tensions between the US and Iran. Iran subsequently launched a missile attack on US military forces based in Erbil and at the Ayn al-Asad airbase in Iraq (with no fatalities).

429. Whilst Iran will probably have sought to re-assess its strategic goals and its regional activities following the killing, the Intelligence Community judged that ***. The Intelligence Community told the Committee that the killing was clearly a very significant event for the Iranian regime alongside the recent domestic protests. These two events have been "*significant drivers of threat*".[309] As the Iranian response to the killing of Soleimani was focused on the US, there is clearly a risk of collateral damage to UK interests given the co-location of US and UK troops in the region, and several groups – particularly Iraqi and Bahraini Shi'a militant groups (SMGs) – could conduct attacks without Iranian approval.

430. If Iran did decide to pursue further retaliation for Soleimani's killing, the Intelligence Community assessed at the time that the most likely methods included: ***

431. When we questioned the Intelligence Community on the extent to which the attack led to an increased threat to the UK, they told the Committee that the immediate attack on the US base was also followed by greater activity by SMGs, not least because the US attack also

[309] Oral evidence – MI5, *** June 2023.

killed Abu Mahdi al-Muhandis, a leader of the Iraqi Shi'a militia umbrella organisation, the Popular Mobilisation Forces, and the founder of Kata'ib Hizbollah. As the Chief of SIS explained:

> *The death of Soleimani meant that the command and control over these militias *** Soleimani was a unique character,* [he] *had this immense authority and was able to hold people in line and call on old favours ***. The militias want Western forces out of Iraq. *** Immediately after the death of Soleimani of course there was some initial activity ... Then in this absolutely heightened paranoia that followed on, as they then expected retaliation, they shot down a civilian airliner ****[310]

How will the threat to UK interests in the Middle East evolve?

432. In 2018, the Intelligence Community assessed – as part of work to determine threats up to 2030 – that the Iranian military threat in the Middle East would increase, which was highly likely to affect UK allies and interests. However, the main determinant remains the bilateral relationship between Iran and the UK. From the evidence we received, it appears that – as with most elements of the Iranian threat – the threat to UK interests could change very rapidly if there were a sudden decline in the bilateral relationship.

433. It was put to us that if Iran were attacked, it would probably not target UK interests militarily unless it assessed direct UK involvement in that attack. We note, however, that even if the UK were not directly involved, there would be a significant risk of misattribution given Iran's deep suspicion of the UK. There would also be a high risk of UK forces in the Middle East being attacked due to their co-location with US forces. In responding to any military attack, Iran could deploy a range of capabilities – this would be particularly aggressive if a large number of Iranians were killed. Its risk appetite for covert operations against UK interests in the region would significantly increase. British nationals across the region and the British Embassy in Tehran would highly likely be at risk, both as a focus for protest and attack. UK vessels in the Gulf could face a significant threat and Iran could also seriously disrupt UK essential services through offensive cyber activity. The response could also include the "*withdrawal of a restraining Iranian hand over Tehran's global network of proxy groups and partners, including, but not limited to, Lebanese Hizbollah, Kata'ib Hizbollah and Asaib Ahl Al-Haq*".[311] As Iran maintains varying degrees of command and control over its network of aligned militant groups, the risk of miscalculation and unmanaged escalation is high, particularly as these groups frequently conduct ***.

434. It is difficult, however, to predict what would trigger such a sharp escalation in tensions (***). That being said, the Committee considers that the following events could potentially trigger such an escalation: UK-aligned seizures of, or perceived interference with, Iranian assets (for example, maritime vessels); a breakdown in UK–Iranian diplomatic relations; and attacks on Iranian (or Iranian-aligned) interests which are supported by the UK (or perceived to be thus).

[310] Oral evidence – SIS, *** June 2023.

[311] Written evidence – HMG, 20 October 2021.

AAA. The UK has substantial security and commercial interests in the Middle East, which are at risk from Iranian hostile activity, including a physical threat to UK nationals in Iran, a threat to UK maritime and commercial interests in the region, and a security threat in respect of terrorism, increased migration and nuclear proliferation.

BBB. Iran has a broad range of tools it could deploy, including missiles and drones (which it could use against Israel, regional US bases – where UK forces are co-located – and Gulf energy infrastructure), its network of militant and terrorist forces, chemical weapons, offensive cyber and disruption of shipping in the Gulf.

CCC. The Iranian physical threat to UK nationals in the Middle East has increased in the last two years as a result of the internal protests in Iran. Detention remains the primary physical threat to British citizens in Iran, and is heightened in relation to dual nationals – particularly because dual nationality is not recognised by Iran. The threat of arbitrary detention has increased since the recent protests in Iran.

DDD. Whilst it appears relatively unlikely, the British Embassy in Tehran is a potential target for an attack. It may well also be the epicentre of protests in the absence of other Embassies.

EEE. The threat of collateral damage to UK Armed Forces stationed in the region (resulting from misidentification or miscalculation) is the main physical risk to British nationals in the Middle East – outside of Iran – due to their sizeable number and co-location with the more heavily targeted US forces.

FFF. In addition to launching physical or cyber-attacks on UK economic interests in the Middle East, Iran has the capability to disrupt or attack commercial shipping in the region – primarily in the Strait of Hormuz: although it practises its capability to close the Strait, it would be a major step for Iran do so.

GGG. The US killing of General Qasem Soleimani in 2020 appears to be contributing to increased regional instability. The Iranian regime may still be seeking revenge and his death * Iran's control over its network of aligned militant and terrorist groups. Given the risks of misidentification and collateral harm, we believe that this continues to pose a particular danger for UK troops co-located with US forces in the region.**

HOW IS THE UK RESPONDING?

Strategy is not a word that I think has crossed the lips of policy-makers for a while, certainly with relation to Iran … Iran policy over the last 20 years has been a series of crisis management … nobody steps out and says "What is the point? … What is the overarching strategic overview? Where do we want to be in 20 years? Where do we want to be in 15 years? How do we get there?" Because nobody has time.

Professor Ali Ansari

STRATEGY AND POLICY RESPONSE

435. Given its breadth and scale, the national security threat posed by Iran clearly requires a cross-Government approach. During this Inquiry, the Committee explored the extent to which the Government's various policies, strategies and plans were aligned, and whether – taken together – they could be considered to represent a coherent Government response to the Iranian threat.

436. Despite the specific characteristics of the threat posed by Iran, such as its high risk appetite, it nevertheless appears that the Government's approach to the state threat is 'actor-agnostic' – i.e. part of broader work to counter state threats in general, regardless of where these threats come from. When the Committee questioned the Foreign Secretary as to why there was no specific approach to counter the Iranian state threat, he told us that the Government's position was that it must "*be ready to counter state threats from wherever they emanate*". However, he recognised that Iran presented a threat on a "*disproportionate scale*", as one of the top three state threats alongside Russia and China, and he acknowledged to the Committee that applying an actor-agnostic approach to a specific Iranian threat was therefore an "*inherent challenge*".[312]

Is HMG thinking long-term enough?

437. Our External Experts were sceptical as to whether the UK had a strategic approach towards Iran at all. The consensus was that HMG had consistently suffered from a focus on crisis management, driven by concerns over Iran's nuclear programme – to the exclusion of other issues.

438. When we put this to the Intelligence Community, the Deputy National Security Adviser (DNSA) appeared to confirm that HMG took a relatively short-term approach. He described the three key strands co-ordinated by the Cabinet Office as: (i) tracking delivery of HMG's 'Iran Strategy';[313] (ii) more reactive work; and (iii) "*then thinking ... where we need to be kind of six, twelve months hence*".[314] It appears that the Government's definition of longer-term thinking is measured in months, not years – let alone decades, as our External Experts suggested was required. This confirms our External Experts' criticism of the Government's approach as short-termist and reactive.

Policy-taker or policy-maker?

439. Perhaps as a result of this failure to think long-term, our External Experts considered that the UK was largely a 'policy-taker' in respect of Iran, tending to follow the lead of the US. While the External Experts agreed on the importance of the UK co-operating with its international partners, there was concern that "*when we* [the UK] *stress partnership, what we tend to do is outsource the formation of our policy*".[315]

[312] Oral evidence – Foreign Secretary, 6 July 2023.

[313] We outline the 'Iran Strategy' later in the chapter.

[314] Oral evidence – NSS, *** June 2023.

[315] Oral evidence – Sir Richard Dalton, 9 March 2023.

440. Despite this, there was no clear agreement as to the value of a more independent strategy. On the one hand, Professor Ehteshami argued that "*I am not sure there is much value in strategising about Iran … I think we are very much in the terrain of fire-fighting and responding pragmatically*",[316] while Sir Richard Dalton argued that the UK "*needs a strategy towards countries of this significance … British policy should try and give itself a little bit of clear blue water between itself and the United States*".[317]

441. The Committee questioned the Intelligence Community on the External Experts' characterisation of the UK as a 'policy-taker' and the view that HMG lacked a long-term strategy of its own. The DNSA said that "*there are a number of areas in which we are very much policy-makers*"; however, the examples then given were all in the domestic sphere – he pointed to steps taken to build the UK's domestic resilience to state threats and to strengthen legislation, such as the National Security Act 2023.

442. The DNSA acknowledged that "*in the international sphere … it is very complex*" and suggested that the Committee explore this further with the Foreign Secretary, "*because obviously the Foreign Office is leading a lot of that work*".[318] When we questioned the Foreign Secretary, he was keen to impress upon the Committee that the Foreign, Commonwealth and Development Office (FCDO) was doing the long-term thinking required:

> *When I stepped into the department ... I kicked the tyres on this ... what the future might look like ... as the current leaders become old, ultimately pass away, who are the next generation: who are the personalities, what is going to happen? So we are absolutely doing the long-term strategic thinking about that ... but when something is on fire, you also have to do fire-fighting.*[319]

However, while the Foreign Secretary may have started conversations in his department, the Committee has seen no evidence that this has led to concrete outcomes or to a revision of HMG's strategic approach. We consider the various strategies that are in place below.

Overlapping strategies

443. During this Inquiry, the Committee was told that there were four elements to the Government's strategy on Iran:

(i) The 2021 Integrated Review's Middle East and North Africa sub-strategy;

(ii) The 2021 National Security Council Iran Strategy;

(iii) The 2023 (actor-agnostic) Counter-State Threats Strategy; and

(iv) The Intelligence Outcomes Prioritisation Plan.

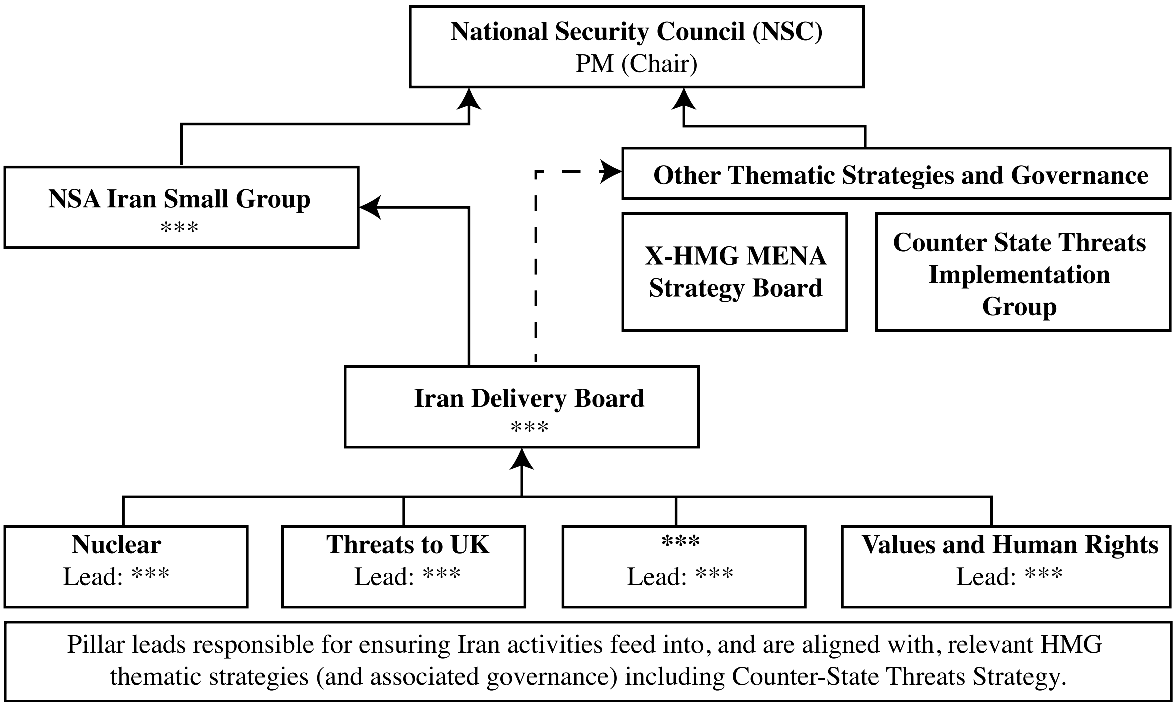
[316] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

[317] Oral evidence – Sir Richard Dalton, 9 March 2023.

[318] Oral evidence – NSS, *** June 2023.

[319] Oral evidence – Foreign Secretary, 6 July 2023.

444. It was not clear exactly how these different strategies and plans fitted together: the diagram below was the best representation of the current governance we were able to establish from the evidence we received. As with our previous Inquiries into national security issues relating to China and Russia, the Government appears to over-complicate its structures and strategies – with the attendant risk of too much talking, at the expense of action.


National Security Council (NSC)
PM (Chair)
NSA Iran Small Group
***
Other Thematic Strategies and Governance
X-HMG MENA Strategy Board
Counter State Threats Implementation Group
Iran Delivery Board
***
Nuclear
Lead: ***
Threats to UK
Lead: ***
***
Lead: ***
Values and Human Rights
Lead: ***
Pillar leads responsible for ensuring Iran activities feed into, and are aligned with, relevant HMG thematic strategies (and associated governance) including Counter-State Threats Strategy.

(i) Integrated Review

445. In March 2021, the UK Government published the Integrated Review (IR)[320] to set the UK's overarching national security and international strategic approach to 2030, and the actions HMG would take to 2025. The IR was somewhat sparse on detail when it came to Iran, mentioning it just five times; however, it set out HMG's key strategic objectives as being:

- to prevent Iran from developing a nuclear weapon; and
- to hold Iran to account for its destabilising activity in the region.

446. The IR noted that Iran is a "*growing threat*" and that, in a context of "*systemic competition*", its "*opportunism* … [is one of the] *key factors in the deterioration of the security environment*". The IR set out that, in response, the UK must improve its ability "*to detect, understand, attribute and act in response to aggression across the range of state threats*". It emphasised the importance of working with allies and partners to ensure greater collective resilience and the ability to act in concert in response to Iranian destabilising activity, as well as to manage any potential escalation. (The importance of the UK Intelligence Community's international partnerships – particularly the US *** – has been a consistent theme during this Inquiry.)

[320] *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, HMG, 16 March 2021.

447. In March 2023, the Government issued a 'Refresh' of the IR.[321] The changes from the 2021 version imply a growing and broader threat posed by Iran, with new specific language on the "*persistent destabilising behaviour of Iran*", explicit reference to increasing physical threats, and mention of concern over growing co-operation with Russia. Meanwhile, language on the nuclear issue may indicate less confidence in the prospect of effective international action on Iran's nuclear programme. The 2021 IR had stated that the UK "*will continue to work with partners on a renewed diplomatic effort to prevent Iran from acquiring a nuclear weapon*"; and that "*the UK will hold Iran to account for its nuclear activity, remaining open to talks on a more comprehensive nuclear and regional deal*". The 'refreshed' version of the IR removed the latter language about remaining open to talks on a nuclear deal, while adding that HMG would seek to "*deter* [Iran's] *destabilising behaviour, including threats against the UK and UK-based individuals*".

448. As well as potentially reflecting HMG's lower confidence in the prospect of effective international action on the nuclear issue – or a reduced willingness to prioritise it – it may be that these changes in the IR Refresh mark a shift in emphasis away from a narrow focus on the nuclear issue, towards addressing the wider holistic threat posed by Iran. Such a shift would be a welcome development; one of the criticisms made by External Experts from whom we took evidence was that HMG needed to develop a more holistic strategy: "*Iran policy has been driven by our nuclear concerns, by the JCPOA* [Joint Comprehensive Plan of Action]. *We need to reverse, I think, the priorities in that sense by having a better understanding of Iran and what it is up to in the whole*".[322] On this point, the Director General MI5 told the Committee that:

> *over the years there have been occasions when it has felt as though Iran is such a complex multi-part problem that the bits of Government that are concerned with domestic risk and the bits of Government that are concerned with nuclear risk have not always felt as coherently joined together as they do now.*[323]

However, he noted that the "*flow of requirements and response*" between the Government's broader strategy and MI5's work on the domestic response to state threats was "*working in my experience, more convincingly now than perhaps at some earlier points in my career*".

Middle East and North Africa sub-strategy

449. To ensure effective implementation of the IR, the National Security Adviser appointed Senior Responsible Owners (SROs) at Director General level across Government to oversee the delivery of each of the IR's 20 sub-strategies. Iran falls under the Middle East and North Africa (MENA) sub-strategy, which is delivered by the FCDO's Director General Middle East and North Africa.[324]

[321] *Integrated Review Refresh 2023: Responding to a more contested and volatile world*, HMG, 13 March 2023.

[322] Oral evidence – Professor Ali Ansari, 9 March 2023.

[323] Oral evidence – MI5, *** June 2023.

[324] At the time this Report was finalised (January 2024), the FCDO reported that this role had been renamed as Director General Afghanistan, Pakistan, Overseas Territories, Middle East and North Africa.

450. At the earlier stages of our Inquiry, the MENA sub-strategy was still being finalised; however, in June 2023 the FCDO provided a summary. It includes three pillars: 'Economic Security'; 'Shared Security and Defence'; and 'Regional Resilience'. The FCDO told the Committee that, in the context of Iran, the 'Shared Security and Defence' pillar is the most relevant. Its objectives are to:

> *strengthen our security and defence partnerships to defend our shared interests from transnational security threats and enhance the region's security, including tackling the upstream drivers of terrorism and working with partners towards durable political solutions to conflicts in the region.*

451. Under this pillar, the FCDO states that, in respect of Iran specifically, it will work *** to:

> *challenge the dangerous trajectory towards nuclear proliferation and find an acceptable regional role for Iran to end its use of hybrid tactics that undermine regional security and the international order.*

While this does still emphasise the nuclear issue, the language indicates that the Government is looking towards developing a broader response across the full spectrum of the Iranian threat.

(ii) National Security Council Iran Strategy

452. In addition to the MENA sub-strategy, which sits under the IR, there is also a separate 'Iran Strategy', as set out by the National Security Council (NSC) – the principal forum through which the Government's objectives with regard to national security are collectively discussed and agreed, and which is chaired by the Prime Minister.[325]

453. In *** 2021 – i.e. predating both the original IR and its 'Refresh' – the NSC agreed the UK's medium-term strategy for Iran, with *** Strategic Objectives, including:

(i) to contain Iran's nuclear ambitions and ensure a non-nuclear armed Iran;

(ii) to encourage Iran to act as a more responsible regional power; and

(iii) to ensure Iran does not pose a direct threat to the UK or the UK's international interests.

454. However, there is no sense from anyone to whom we spoke of: how the NSC Iran Strategy relates to the IR MENA sub-strategy; which of them takes precedence; and whether the NSC Iran Strategy has taken account of the changes in the IR Refresh. It is concerning that these strategies appear not to have been aligned.

[325] The NSC's membership comprises: the Prime Minister, the Deputy Prime Minister, the Chancellor of the Exchequer, the Foreign Secretary, the Home Secretary, the Defence Secretary, the Secretary of State for Energy Security and Net Zero, the Secretary of State for Science, Innovation and Technology, the Attorney General, the Security Minister and the Minister of State for Development and Africa. When required, other Cabinet Ministers, the Agency Heads and the Chief of the Defence Staff may also attend.

455. The same Director General in the FCDO (Director General Middle East and North Africa) is responsible for the Iran Strategy as for the MENA sub-strategy, reporting to the Foreign Secretary and chairing a Board which the Committee was told "*covers the sort of wider Middle East and North Africa region but including the Iran Strategy, and that group ... it drives delivery*".[326] The Committee was also told that the FCDO has a dedicated Iran Unit, which co-ordinates cross-Government activities in line with the objectives set by the NSC, and that the Head of the Iran Unit chairs monthly cross-Government delivery boards to oversee delivery and manage emerging risks.

456. The Committee was originally told that the Iran Strategy is being implemented through a 'Campaign Model', to ensure a joined-up cross-Government approach (previously known as Fusion Doctrine) and strengthen collective oversight and co-ordination of Iran work, by focusing activity clearly on strategic outcomes and the effective monitoring and evaluation of their delivery across Government. The Committee was told that officials across all relevant Whitehall departments worked together to develop the structure and process by which the Iran campaign model is being implemented. We return later to the question of whether the structures and processes in place are driving change.

457. In *** 2021, eight 'Strategic Campaigns' (set out below) were signed off as forming the NSC Iran Strategy. Each 'campaign' describes the 'theory of change' for the respective priority policy area, from overarching goals, through the outcomes HMG wants to achieve, to the implementation and delivery of identified outputs. Each campaign is supported by targets, key performance indicators, and enhanced monitoring and evaluation. The Committee was told that the campaign model seeks to ensure that workstreams outside of the *** Strategic Objectives agreed by the NSC – such as nuclear, regional and state threat – also receive attention. Originally, the Committee was told that there are regular Campaign Board meetings to co-ordinate delivery of the campaigns, and that delivery was overseen by the National Security Implementation Group (NSIG) on Iran (NSIGs are explained later in this chapter). However, at the point at which this Report was finalised (January 2024), HMG advised that NSIGs had been renamed in 2021 as 'Integrated Review Implementation Groups' (IRIGs), but then – confusingly – that, as of the 2023 IR Refresh, "*some IRIGs continued to use that title, others did not*".[327] There appears to be very little clarity around structures: while renaming may be of little practical consequence, it is unnecessary to muddy the waters. It must be clear who is responsible for delivery.

[326] Oral evidence – HSG, 6 July 2023.

[327] Written evidence – HMG, 8 December 2023.

The eight Strategic Campaigns

Strategic Campaign	***Detail***	***Lead***
New Settlement	***	***
Counter Nuclear Proliferation	***	***
Regional Security	***	***
Protect the UK and its Interests	***	***
Raising the Cost	***	***
Dual Nationals	***	***
Force for Good	***	***
Enabling the Relationship	***	***

458. However, in June 2023, the FCDO provided the Committee with evidence that "*in light of the changing context, the NSC agreed* [a number of] *HMG objectives for Iran in *** 2023. These ... form the basis of the new pillar structures driving delivery of the NSC agreed approach*". Effectively, therefore, the eight 'Strategic Campaigns' have – just two years later – been subsumed into four pillars. For instance, the 'Raise the Costs' and 'Protect' campaigns "*are being essentially subsumed into one campaign reflecting ... that they are both aimed at reducing the threat to the UK*".[328] The Foreign Secretary told the Committee that he felt that this "*distilling down*" was beneficial for HMG's approach: "*I welcome going from eight to four ... less complicated is better*".[329]

459. The four new pillars are as follows (with the nuclear issue remaining a priority), ***:

Pillar	***Detail***
Nuclear	***
Threats to the UK	***
***	***
Values and Human Rights	***

[328] Oral evidence – HSG, 21 June 2023.
[329] Oral evidence – Foreign Secretary, 6 July 2023.

460. The Chief of SIS told the Committee that he welcomed this clearer prioritisation he had received from the NSC: "*Nuclear *** and then there has been sort of competing demands around of course *** regional behaviours, but nuclear ***. So I feel like I have a clear prioritisation*".[330] The Home Secretary agreed, telling the Committee that it struck "*the right balance*", *** underlining the importance of the 'Protect' element in the context of the increase in the Iranian threat and activity in the UK.[331]

461. Leaving aside the numbers, we note that there was no explanation of why the previous 'Campaign Model' is now a 'Pillar Model' – or if that makes any actual difference other than semantically. We also note that it remains difficult to determine accountability: as with any strategy, it should be clear who is responsible for driving implementation, and whose performance rating and pay rewards will be determined by its success or failure.

462. When the Committee questioned the DNSA as to whether that work was being overseen at the centre of Government, we were told that, over the course of the six months to June 2023:

> *we have had several sessions with Ministers over that period of time. We have had several meetings with the Prime Minister to inform him of implementation against the NSC objectives and some of the live issues that we are seeing and, from an official perspective, I would say that we are meeting every fortnight.*[332]

463. However, in terms of the NSC's oversight of its Iran Strategy, we note that the NSC does not appear to have met regularly to discuss Iran specifically; when we questioned the Home Secretary on how often the NSC had met to discuss Iran during her ten-month tenure, she told us that "*I couldn't be sure, if I am honest …****."[333] The DNSA informed the Committee that "*the last* [NSC] *meeting* [on Iran] *was* ***"[334] – which we were later told had taken place ***. It is surprising that the NSC has met only *** to discuss Iran. The DNSA told us that the NSC's role was to ensure "*a coherent approach balancing, you know, all of* [the] *various different equities*".[335] However, we are concerned as to how it can be doing so without regular discussion.

[330] Oral evidence – SIS, *** June 2023.
[331] Oral evidence – Home Secretary, 6 July 2023.
[332] Oral evidence – NSS, *** June 2023.
[333] Oral evidence – Home Secretary, 6 July 2023.
[334] Oral evidence – NSS, *** June 2023.
[335] Oral evidence – NSS, *** June 2023.

(iii) Counter-State Threats Strategy

464. Despite the MENA IR sub-strategy and the NSC Iran Strategy, as we noted previously much of the Government's work to counter the state threat is actor-agnostic. This is set out in the 2023 Counter-State Threats Strategy (CSTS), which considers state threats thematically rather than geographically (i.e. 'actor-agnostic') and is overseen by the Deputy Prime Minister in the Cabinet Office. We note that the CSTS was first mentioned to the Committee in 2019 – over four years ago: it has taken a surprisingly long time to develop.

465. The Committee requested on several occasions that the CSTS be shared with the Committee as part of this Inquiry. The DNSA eventually committed to share it with us; however, disappointingly, HMG still did not provide this to the Committee before we finished writing this Report, nor did it provide an adequate explanation for its failure to do so. This is unacceptable. As a result, we have been unable to scrutinise the Government's counter-state threats strategy as part of this Inquiry into one of the key state threats.

466. The DNSA did describe the overarching objective of the CSTS to the Committee, saying that it was to enable HMG "*to drive activity from a kind of threat-agnostic perspective to improve, you know, our resilience to all of those kinds of threat vectors ... we want to improve the resilience to these threats writ large*".[336] We recognise the value of an actor-agnostic strategy, but are not clear how it can work alongside existing Iran-specific strategies and approaches, or whether Iran will receive sufficient priority when set against the Chinese and Russian state threats.

467. HSG saw the value of the CSTS as "*pulling in ... non-traditional parts of Government who haven't always been part of the national security community to really bring really strong effect here*".[337] However, as this Committee made clear in our *China* Report, policy departments charged with security matters do not necessarily have sufficient resources, expertise or knowledge to investigate and counter state threats.

[336] Oral evidence – NSS, *** June 2023.

[337] Oral evidence – HSG, 21 June 2023.

(iv) The Intelligence Outcomes Prioritisation Plan for Iran

468. The Intelligence Outcomes Prioritisation (IOP) process establishes the intelligence required from GCHQ and SIS to help deliver the policy strategies set out above.

The IOP process

The Committee was previously told that, under the IOP process, each NSIG establishes the intelligence it needs in order to deliver its policy outcomes, and prioritises these requirements in an IOP Plan.

NSIGs were officials' meetings, accountable to the NSC for the implementation of the Government's strategy with regard to the highest-priority thematic and geographical challenges relating to UK national security. NSIGs sought to improve cross-Government co-ordination without centralising the response. Each NSIG was led by an official SRO. There was not a set number of NSIGs – they were created and disbanded according to NSC priorities. The Committee was told that, as of 2021, NSIGs had been renamed as IRIGs. However, since 2023 this name itself appears to have fallen out of use, with a subsequent vague description of "*senior official groups*".

Once each of these "*groups*" has prioritised intelligence requirements in an IOP Plan, each IOP Plan is then taken to the Joint Prioritisation Committee (JPC) for discussion. The JPC is chaired by the DNSA and the JIC Chair and the FCDO's Director General Defence and Intelligence. The JIO assists by examining the policy outcomes within each IOP Plan to assess what level of understanding can be provided by different sources (including secret, open, diplomatic, academic and business sources). This helps to establish where secret intelligence is vital and where it could possibly be replaced by open source work.

Having reviewed the IOP Plans for the different "*groups*" and taken into account ministerial priorities and the potential impact of changes in allocation, the JPC then recommends to the NSC the appropriate balance of Agency effort for the forthcoming year for each IOP Plan.[338] This process is designed to ensure that GCHQ and SIS's work[339] accords with the priorities set by the NSC, and demands from 'customer' departments in Government. GCHQ and SIS are held accountable for delivery against intelligence requirements by the Foreign Secretary in their ministerial oversight role as mentioned above, and by the National Security Adviser in their role as principal Accounting Officer for the Agencies.

[338] If an SRO realises that they need additional effort midway through the year, they can bid for it as a reprioritisation. If the SRO thinks that this reprioritisation will be a long-term requirement then it will have to be considered as part of the annual round.

[339] As MI5 is self-tasking, it is not included in this process.

469. GCHQ explained to the Committee that, in delivering its IOP requirements:

> *within the three Agencies, we have a regular set of meetings at all levels … to both co-ordinate and monitor the delivery against those intelligence outcomes priorities … a regular meeting with … opposite numbers … and then on a *** basis we do what we call a *** Review, which is to look at each of the different threat areas or target areas and see how we are delivering against those intelligence outcomes.*[340]

470. The 2021 IOP Plan for Iran is below.

***

Coverage versus effects

471. SIS and GCHQ's intelligence work encompasses both 'coverage' and 'effects'. 'Coverage' is the collection of information (or acquisition of information from allied intelligence services) by the Agencies, whereas 'effects' describe the Agencies' engagement in activities which have real-life outcomes. One example of effects work might be ***. Another might be SIS ***.

The roles of SIS and GCHQ

SIS is the UK's foreign human intelligence (HUMINT) agency. Areas of work which SIS undertakes include:

- cultivating and maintaining agents who are in a position to pass on secret information; and
- obtaining and sharing information which our allies have gathered on Iran.

GCHQ is the UK's signals intelligence (SIGINT) agency. Areas of work which GCHQ undertakes include:

- the bulk interception of communications for analysis and intelligence reporting;
- intercepting material transmitted over military communications systems;
- covertly accessing computer systems in order to obtain the information they contain; and
- sharing information with our allies' intelligence agencies.

[340] Oral evidence – GCHQ, *** June 2023.

472. We note that the IOP Plan outcomes appear to relate *** coverage, *** effects. We questioned the Agencies on the extent to which they carry out *** operations under the IOP Plan, and on the balance of effort between their coverage and effects work. The Chief of SIS explained that he prioritised ***:

> *Always, if a choice has to be made, I will put resources on ensuring we get *** ... a significant amount of resource goes on ***. *** ... we have to focus quite hard, given the prioritisation on that, to where we can *** ... our ability to *** is not in the same place* [as it has previously been ***] ... *and in other areas our ability to ***.*[341]

473. In terms of what effort is devoted to effects work, GCHQ told the Committee that:

> *we do obviously prioritise our* [effects] *efforts against those things which are most, you know, critical to the UK ... the Iranian threat *** is much less than the Iranian *** so we would prioritise *** on that threat rather than the *** threat.*[342]

474. While the IOP Plan *** for effects work, GCHQ told the Committee that "*our effects work also gets inputs from other mechanisms, so the *** which articulates the priorities for effects work that GCHQ undertakes with ***. So the IOP is not the only articulation of what we are trying to do to respond*".[343] This is reassuring; however, we question accountability mechanisms for effects work undertaken outside of the framework of the IOP Plan. (We consider specific case studies demonstrating effects work later in the Report. This includes – for example – Operation *** in the chapter on ***, Operation *** in the chapter on ***, and Operation *** in the chapter on ***)

*Understanding Iran's ****

As an example of the IOP process in action, we were told that the Intelligence Community had sought to include an additional intelligence requirement in the 2022 Iran IOP Plan, for SIS and GCHQ to inform HMG's understanding of Iran's ***. As such, in the 18 months prior to August 2023, the Intelligence Community had "*delivered a small body of reporting*" on ***, which has contributed to HMG's broader understanding of ***.

We welcome this requirement in the 2022 Iran IOP plan as a step in the right direction. Given that the *** to the UK, this should have been given priority previously. The importance of understanding Iran's *** was illuminated starkly by Iran's ***, as explored in the Threat section of this Report.

[341] Oral evidence – SIS, *** June 2023.

[342] Oral evidence – GCHQ, *** June 2023.

[343] Oral evidence – GCHQ, *** June 2023.

Tri-Agency co-ordination

475. While the IOP Plan sets requirements specifically for GCHQ and SIS, the Committee was told that GCHQ, SIS and MI5 work together on the cross-Agency 'Iran Mission'. The Committee was told that the Iran Mission:

> *deals with threats from Iran such as:*
>
> - *its espionage activity;*
> - *its intent to target dissidents and oppositionist political groups around the world;*
> - *its use of offensive cyber operations; and*
> - *Iran's use of partners and aligned groups to respond asymmetrically to perceived hostile action taken against Iran.*[344]

476. While the 'Mission' appears to be articulated, we note that there is no tri-Agency plan as such. During our Inquiries into national security issues relating to Russia and China, the Committee was told that a tri-Agency approach existed to co-ordinate work across the three Agencies. We questioned why there was no plan on Iran. GCHQ responded: "*basically because we don't see we need it. Because there is a very clear national strategy and actually that we have been working on Iran collaboratively and quite effectively for a number of years ... that would be adding an extra level of governance that is not necessary*".[345]

477. When we questioned Ministers on this, the Foreign Secretary also told the Committee that he did not consider a tri-Agency plan to be required and that the FCDO-based Iran Unit provided "*a lot of cross-Whitehall co-ordination ... the division of labour, as it were, on this I think is pretty clearly defined ... I am not feeling that there is a gap that needs filling in terms of the co-ordination between the various bits of the system*".[346] Similarly, the Home Secretary told us:

> *In terms of MI5's integration with SIS and the other agencies, I mean MI5 has a dedicated Iran mission ... they benefit from very meaningful co-operation and access to information and tools from across UKIC* [UK Intelligence Community]*, Counter Terrorism Policing and the broader Government community ... so I think that MI5 is playing a very full role and is highly connected to other partners in meeting the threat posed by Iran.*[347]

Co-ordination with DI

478. DI is tasked through a process it runs called the Defence Strategic Intelligence Prioritisation Process. Through this process, DI works with officials from the wider Ministry

[344] Written evidence – HMG, 27 October 2021.
[345] Oral evidence – GCHQ, *** June 2023.
[346] Oral evidence – Foreign Secretary, 6 July 2023.
[347] Oral evidence – Home Secretary, 6 July 2023.

of Defence (MoD) to identify the supporting intelligence requirements for the MoD's Military Strategic Objectives. (The Military Strategic Objectives are identified and prioritised via the MoD's Strategic Effects Management Process.)

479. When the Committee asked how DI ensures that its efforts are co-ordinated with the three Agencies, we were told that DI attends the JPC meeting which examines the IOP Plans, and aligns its collection activity with decisions made at that meeting: "*whilst we are not formally part of the *** Review process within UKIC, you will see constant contact between the teams at every level and their UKIC counterparts*". The Deputy Chief of Defence Intelligence (CDI) also told us that he frequently attends the Agencies' top-level governance body ***.[348]

HHH. The Government's policy on Iran has suffered from a focus on crisis management, driven by concerns over Iran's nuclear programme, to the exclusion of other issues.

III. 'Fire-fighting' has prevented the Government from carrying out longer-term thinking and developing a real understanding of Iran and the complexity of the problem. The Government must stop its short-termist, reactive approach: 'longer-term' must mean the next 5, 10 and 20 years, not 6 to 12 months.

JJJ. We welcome the increased focus on Iran in the 2023 Integrated Review Refresh. However, as with our previous Inquiries into national security issues relating to China and Russia, the Government appears to over-complicate governance structures and strategies – with the attendant risk of too much talking, at the expense of action.

KKK. There is no sense from anyone we spoke to of: how the National Security Council Iran Strategy relates to the Integrated Review Middle East and North Africa sub-strategy; which of them takes precedence; and whether the National Security Council Iran Strategy has taken account of the changes in the Integrated Review Refresh. It is concerning that these strategies appear not to have been aligned.

LLL. It remains difficult to determine accountability for the National Security Council Iran Strategy – as with any strategy, it should be clear who is responsible for driving implementation, and whose performance rating and pay rewards will be determined by its success or failure.

MMM. We note with concern that the National Security Council met * to discuss Iran. If the National Security Council is to have an 'Iran Strategy', then it should be ensuring implementation of it, through regular discussions with the officials responsible.**

[348] Oral evidence – DI, *** June 2023.

NNN. The Counter-State Threats Strategy has taken four years to develop – whilst this is an extraordinarily long time to wait for such a key piece of work, the Committee cannot provide Parliament or the public with any assurance that it was worth the wait: the Government failed to provide the Committee with the Strategy. We regard this as completely unacceptable: this Committee has been given the statutory responsibility to oversee such matters, and we question what the Government's reasons are for withholding it.

OOO. While we recognise that there will be some elements of the state threats from China, Russia and Iran that are broadly similar and which will benefit from an actor-agnostic approach, there will be fundamental differences which could be overlooked. The Iranian threat is quite different in many respects and it is essential that it receives sufficient priority, and that Russia and China do not dominate the Government's focus.

PPP. The Intelligence Outcomes Prioritisation Plan – which sets the requirements for GCHQ and SIS – * 'coverage' *** 'effects'. We recognise the need to prioritise *** and the relatively ***. Nevertheless, proper consideration must be given to ***.**

QQQ. It is a step in the right direction that the Intelligence Outcomes Prioritisation Plan in 2022 introduced a requirement to provide greater understanding of Iran's *.**

MINISTERIAL RESPONSIBILITIES

480. We have mentioned the role of the National Security Council (NSC), under the Prime Minister's chairmanship, in relation to Government policy on Iran. The Foreign Secretary and the Home Secretary sit on the NSC, and both have specific responsibilities in relation to work on Iran and statutory responsibilities in relation to the Intelligence Community.

Foreign Secretary

481. The Foreign Secretary is responsible for managing the UK–Iran bilateral relationship, engagement with international counterparts, and policy on Iran. He also has oversight of GCHQ and SIS and responsibility for the National Cyber Force.

482. In terms of the UK–Iran bilateral relationship, the Foreign Secretary told the Committee that there had been a lack of engagement with his Iranian counterpart:

> *I met Abdollahian when I was a regional minister before I became Secretary of State.*[349] *I didn't reach out to him upon my appointment and I have heard back that there is disappointment in the Iranian system that I've not tried to build a relationship with Abdollahian; whilst, simultaneously, they have significantly escalated their state threat activity against us ... it strikes me there is a real disconnect.*[350]

We were surprised that there appeared to be such limited interaction at Ministerial level in comparison with his predecessors, since these channels can be useful to deliver messaging to deter malign activity, and reduce the risk of misunderstanding and unintended escalation.

483. The Foreign Secretary does discuss Iran with his international counterparts, including policy on nuclear, regional stability, destabilising behaviour and human rights. The Foreign Secretary told the Committee that Iran-related work took up "*a significant minority of* [my overall] *time*", ranking it third behind work on Russia/Ukraine, and work on China and the Indo-Pacific tilt. He described Iran as "*subordinate to those two in terms of time allocation but not far off the pace – and then there is probably a gap and then any other given file is quite a long way behind it*". He told the Committee that he received secure briefings "*at least once, often multiple times in the week*", and that – perhaps given the unpredictable and often acute nature of the threat from Iran – "*Iran is one of the top three things that I am briefed on*", second only to the situation in Ukraine.[351]

484. As noted above, the Foreign Secretary has statutory responsibility for GCHQ and SIS and we therefore questioned how often he met with Agency Heads and received such briefings from them directly. The Chief of SIS told us that "*it would be very surprising if I would go*

[349] The Foreign, Commonwealth and Development Office (FCDO) subsequently clarified that the Foreign Secretary did not meet Foreign Minister Hossein Amir-Abdollahian when he was a regional minister, but met Iran's Deputy Foreign Minister, Ali Bagheri Kani, in 2021.
[350] Oral evidence – Foreign Secretary, 6 July 2023.
[351] Oral evidence – Foreign Secretary, 6 July 2023.

for a month or so without sitting down with the Foreign Secretary".[352] However, the Foreign Secretary thought that their meetings were less frequent: "*I have met with* [the Chief of SIS] *I think half a dozen times, seven times, since being appointed as Secretary of State*" (i.e. approximately once every two months). In terms of meetings with the Director of GCHQ, he thought these took place "*probably slightly less ... but not far off. So again, at or near half a dozen times*". He told us that Iran was "*always on the agenda*" at every meeting and that it inevitably formed a significant part of his conversations with Agency Heads, particularly on the subjects of nuclear and state threats, which "*dominate*".[353] The Committee was nevertheless surprised by the relative infrequency of such meetings.

485. In addition to that general oversight, the Foreign Secretary also has statutory responsibilities in terms of authorising GCHQ and SIS activity. The Foreign Secretary is formally consulted by SIS and GCHQ for approval of operations in three different ways – warrants, authorisation and submissions. The Foreign Secretary's primary involvement with SIS and GCHQ day to day is through his role in authorising warrants (legally the most intrusive actions of SIS and GCHQ).[354] The Foreign Secretary told us: "*I suspect that I probably do around ... *** warrants a month*",[355] of which "*around ***% ... relate solely or primarily to Iran*".[356] This does not, however, include "*a number of, you know, *** type warrants which will have Iran stuff embedded within it*".[357] This is fewer than the warrants authorised relating to Russia (around ***%) and China (around ***%) respectively. The Foreign Secretary told the Committee that he had not refused an Iran-related warrant from GCHQ or SIS.

486. The Foreign Secretary is also jointly responsible, with the Defence Secretary, for the National Cyber Force (NCF) – a partnership between GCHQ and the Ministry of Defence (MoD) primarily (although it also includes elements from SIS and the Defence Science and Technology Laboratory). Given the threat posed by Iran's cyber capability, the NCF has a vital role to play in the UK's response. Activity undertaken by the NCF is approved jointly by the Foreign Secretary and the Defence Secretary. We challenged the Foreign Secretary as to whether this dual arrangement – somewhat unusual in Government – was effective. He told the Committee:

> *I have not yet been confronted with an example of it not working ... I think the clear prioritisation that has come out of the NSC and the IOP* [Intelligence Outcomes Prioritisation] *would minimise the risk of disagreements like this ... this is always an evolutionary process ... but we have not been confronted with that at this point.*[358]

[352] Oral evidence – SIS, *** June 2023.

[353] Oral evidence – Foreign Secretary, 6 July 2023.

[354] These warrants cover: interception of communications; intrusive surveillance (in a private, rather than a public, space); interference with property; equipment interference ('hacking'); and obtaining and examining bulk personal datasets.

[355] Oral evidence – Foreign Secretary, 6 July 2023.

[356] Written evidence – Foreign Secretary, 25 July 2023.

[357] Oral evidence – Foreign Secretary, 6 July 2023.

[358] Oral evidence – Foreign Secretary, 6 July 2023.

Home Secretary

487. The Home Secretary is responsible for the domestic security of the UK. Within this wide remit, her responsibilities which directly relate to Iran include:

- Policy responsibilities, such as:
  - – the domestic response to state threats;
  - – investigatory powers policy;
  - – preventing terrorism; and
  - – tackling cyber-crime (which is a vector by which Iran conducts some of its cyber activity).
- Delivery responsibilities, such as:
  - – the use of legislative tools such as proscription, and the operation of the National Security Act 2023 regime, which seeks to modernise counter-espionage laws and make the UK a harder operating environment for state and state-directed actors;
  - – the operation of the UK's immigration and visa regime, which is used to limit malign actors' access to the UK, including Iranian state actors and aligned individuals and groups;
  - – co-ordinating the operational response to domestic national security incidents; and
  - – playing a key role in the delivery of the National Cyber Strategy.
- Ministerial responsibility for oversight of MI5 and the National Crime Agency, which includes statutory responsibility for considering and authorising warrants in relation to a range of covert intelligence-gathering activities.[359]

488. We cover the Home Office's activities to protect the UK's domestic security in a later chapter ('Defending the UK'); however, we note that, in speaking to the Home Secretary, it appeared from her responses that much of the operational detail was overseen by the Security Minister. The Home Secretary reassured the Committee as to her involvement, but added that the Home Office was:

> *good at announcing new plans and strategies ... but actually delivering outcomes is what I want to be judged on ... who has responsibility for that? I mean ultimately, I do ... The Security Minister is involved at a more kind of operational level, I would say, at driving through some of these strategies and*

[359] The Home Secretary's statutory responsibilities in relation to warrantry are set out in the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. The Home Secretary also has oversight of policing in England and Wales, and also considers and approves warrants from policing, the National Crime Agency, His Majesty's Revenue and Customs, and a number of other organisations involved in the Government's response to the Iranian threat.

> *making these plans a reality ... Ultimately, the responsibility lies with me ... but ultimately my diary doesn't allow me to do that and his does ... all of his time will be spent on the Homeland Security Group action plans and delivery plans that we have and working with officials on the detail on a weekly basis in a way that I wouldn't be doing and then I will have updates and come in at strategic points.*[360]

489. MI5 does not 'report' to the Home Secretary in the way that GCHQ and SIS do to the Foreign Secretary (being tasked Agencies). It is operationally independent (although it does update the Home Secretary regularly on operational matters). Nevertheless, the Home Secretary is legally required to authorise specific covert activity. The Committee was told that, in relation to its Iran work, MI5 submits warrants to the Home Secretary to take intrusive action on individuals in the UK assessed to be agents or proxies operating on behalf of the Iranian Intelligence Services (IIS). From 22 October 2022 to 12 July 2023, the Home Secretary considered *** warrants relating to Iran (out of *** warrants across all counter-state threats).

490. We questioned how often the Home Secretary was briefed by MI5 on Iran-related issues. Director General MI5 told the Committee that he would:

> *typically on a weekly basis brief the Home Secretary on what we were seeing and if the content of those investigations throws up policy-relevant choices, prioritisation decisions, legislation angles ... we would feed those thoughts to our colleagues and they then take forward the sort of wider system response, while we get on with the operational investigations.*[361]

The Home Secretary told the Committee that national security work was her top priority, but that:

> *I wouldn't say Iran is coming up every week in my operational meeting with MI5 ... I would say, every other week ... but we also have Ministerial assurance groups that I chair with MI5 and oversee more strategic work by MI5 and others, and Iran does constitute an appropriate part of that.*[362]

The Home Office subsequently clarified that the Home Secretary receives regular updates on Iran in MI5's weekly letter.

RRR. We are concerned by the lack of engagement between the Foreign Secretary and his Iranian counterpart; Ministerial channels can be useful in delivering messaging to deter malign activity, and to reduce the risk of misunderstanding and unintended escalation.

SSS. We are surprised at the relative infrequency of meetings between the Foreign Secretary and the Heads of GCHQ and SIS, compared to the greater engagement by previous Foreign Secretaries.

[360] Oral evidence – Home Secretary, 6 July 2023.

[361] Oral evidence – MI5, *** June 2023.

[362] Oral evidence – Home Secretary, 6 July 2023.

RESOURCING, PRIORITISATION AND EXPERTISE

491. The amount of effort and resourcing allocated to work by the Agencies to counter the Iranian threat has fluctuated in recent years (which aligns with evidence the Committee received from External Experts that the Government's response to the Iranian threat has been short-termist). Overall, however, the trend – at the time the Committee took evidence for this Inquiry – appeared to be a decline in resourcing on Iran in comparison with the Agencies' other areas of work.

492. When we questioned the Foreign Secretary on this, he told the Committee that resourcing on Iran had "*rebalanced*" following the conclusion of the Joint Comprehensive Plan of Action (JCPOA) negotiations, and that, in his view, the current level of resourcing "*does feel about right*" – although he noted the possibility that unexpected events might shift Iran's posture towards the UK, and this would affect the amount of resource required.[363] We questioned the Intelligence Community on the resourcing each organisation has allocated to work on the Iranian threat, and how this has changed in recent years.

GCHQ

- The number of GCHQ staff dedicated to work on Iran fell by *** between 2015 and 2021 – from *** to *** staff.
- As a proportion of GCHQ's total operational resourcing, this fall is *** – from ***% to ***%.
- Approximately half of this decline occurred between ***, from *** staff dedicated to Iran to *** (as a proportion of GCHQ's total operational resourcing, from ***% to ***%). Some reduction that year was to be expected, given the conclusion of the JCPOA negotiations with Iran during that period.
- In ***, investment on Iran-related work was also reduced by approximately ***, to enable greater investment in the *** and *** campaigns.
- Perhaps as a result of this earlier reduction, in *** GCHQ was required to increase ('surge') resource on Iran from *** to *** staff. We note that surge staff are temporarily allocated ***.
- Between ***, the number of dedicated staff once again then declined, from *** staff to *** (as a proportion of GCHQ's total operational effort, from ***% to ***%).

493. GCHQ noted that the impact of the *** in staff allocation since 2015 had been "***", although we were not provided with more detail on how exactly that impact was seen. As a result of the reduction, GCHQ's efforts since have focused on "***" – which appears to imply that GCHQ is ***.

[363] Oral evidence – Foreign Secretary, 6 July 2023.

494. GCHQ told the Committee that, despite the reduction in the number of analysts, it had nevertheless invested significantly in its Iran-related capabilities and partnerships in 2019. GCHQ also told the Committee that:

> *we have worked hard to preserve a lot of our expertise. So we have a *** team that looks at *** and has that technical expertise ... we have also maintained a significant level of investment in Farsi language. We have approximately *** Farsi linguists at the moment. So despite the overall decrease, we have managed to maintain, I think, some of these key skills.*[364]

GCHQ said that this had enabled it to produce a level of intelligence on Iranian threats "*more impressive than those numbers would suggest*", and assured us that this meant that GCHQ's intelligence represented "*good value for money*" as well as a "*good level of coverage*".[365] This sense of "more for less" is reassuring – however, the overall decrease remains of concern, particularly given the significance of the Iranian cyber threat.

MI5

- MI5's work on the Iranian threat is primarily included under its broader 'Counter State Threats' mission. In March 2021, the number of full-time equivalent (FTE) staff working on the overall 'Counter State Threats' mission was ***. This represented ***% of MI5's total staffing numbers.
- As of September 2021, staff dedicated to Iran made up ***% of the total number of staff within the 'Counter State Threats' mission – approximately *** FTE.
- As of October 2021, Iran-related investigations made up around ***% of MI5's Counter State Threats investigations. Staff working in the Iran Mission have access to the specialist covert intelligence collection teams which provide, for example, surveillance or technical capability, and to a range of analysts and assessment capability. The proportion of this resource available to the Iran Mission is prioritised in line with the level of national security threat posed by Iran.
- Work on Iran is also covered under the Protective Security mission, which includes the work of the National Protective Security Authority – although this is actor-agnostic rather than targeted specifically against Iran.

495. As previously noted in the Committee's *Russia* Report, 25 years ago MI5 devoted around 20% of its effort to Hostile State Activity (which includes Iranian activity alongside the hostile activity of such states as Russia and China). This allocation of effort declined, as the terrorist threat grew. Specifically, ***. The Director General noted that MI5 "*did not have other options*" but to increase its resourcing on counter-terrorism ***:

[364] Oral evidence – GCHQ, *** June 2023.

[365] Oral evidence – GCHQ, *** June 2023.

> *We had to dispose our resources in the least worst way available. Part of that – not something we would have chosen to do, other things being equal – was to pare back the amount of dedicated resource we had on* [state threats] *** *at that time.*[366]

496. Since 2017, MI5 has "*begun to restore* [its] *Iran mission to previous staffing levels*", and created three teams focused on the threat ***. While resourcing has grown as Iranian hostile activity has grown, the Director General acknowledged that this was "*not as dramatically as in an ideal world*". Nevertheless, he noted that work relating to Iran had commanded:

> *a substantially larger share of ... ***, the teams who are not dedicated to any particular threat but do ***. Because of the intensity of the Iranian threats to life in particular, ***.*[367]

497. While the Director General agreed with the Committee that, if there were to be an increase in overall resources, there would be scope for MI5 to do still more, the Home Secretary told the Committee that she was confident that the level of resource allocated by MI5 was appropriate: "*it would be proportionate, based on the threat that is posed ... they tell me when they are* ***".[368] Nevertheless, MI5's assessment was that it is currently "***", that balancing its state threats work with its counter-terrorism is "***", and this has led to "***".[369] As we reported in our *Extreme Right-Wing Terrorism* Report, MI5 has not received an increase in resources commensurate with the increased range of issues it is responsible for countering. As the Committee called for in that Report, MI5 must be given additional funding to enable it to counter this increased range of issues without other areas of work suffering as a consequence.

498. Due to MI5's need to "*rigorously prioritise*" threats from the Iranian Intelligence Services (IIS), it focuses its investigative and operational resources on those investigations ***, and investigations which provide opportunities ***. In practice, this means that MI5's investigative and operational work is "***".[370]

SIS

- SIS told us that its total staffing on the Iran nuclear issue had reduced *** between *** and ***, following the signing of the JCPOA ***.
- Nevertheless, the overall number of SIS staff dedicated to Iran has risen consistently between *** and *** – from *** to *** FTE staff. SIS's total allocation of effort on Iran also rose consistently between *** and *** – from ***% to ***%.
- Since ***, there has been a decline in personnel working on Iran, from *** FTE staff to *** in 2021.

[366] Oral evidence – MI5, *** June 2023.
[367] Oral evidence – MI5, *** June 2023.
[368] Oral evidence – Home Secretary, 6 July 2023.
[369] Oral evidence – MI5, *** June 2023.
[370] Oral evidence – MI5, *** June 2023.

499. The Chief of SIS compared the level of resourcing allocated to Iran with other areas of work:

> ***.[371]

500. The reduction in staffing on the Iran nuclear issue is of concern, and may have been premature, given that Iran has consistently breached its commitments ***. We questioned whether SIS has capacity to meet its nuclear-related requirements ***, but the Chief of SIS appeared relaxed, telling the Committee:

> *in the heady days of the ***, it seemed sensible to move off and focus on other things but that optimism was punctured some time ago, so we have reasserted that as a priority ... I am comfortable that, against the other priorities imposed on us by intelligence customers, that we have the level of staffing on Iran about where it should be.*

Although he qualified that:

> ***.[372]

DI

- Within DI, *** analysts spend over half of their time on Iran, and a further *** analysts contribute but spend less than half of their time on Iran.

501. DI cites Iran as a "*Top Priority*" alongside Russia and China (although we note ***). In terms of resourcing focused specifically on Iran's nuclear programme, the Chief of Defence Intelligence (CDI) told us that DI's *** had remained at a broadly similar level in recent years, and he was confident that DI retained sufficient technical and subject expertise (for example, on nuclear and weapons systems).[373]

JIO

- The JIO's Middle East team currently includes *** and *** posts exclusively focused on Iran.
- Other analysts across the JIO work on Iran-related assessment as part of their other specialisms (for example, state threat activity, economics, weapons and counter-proliferation).

HSG

- In September 2021, the Home Office established a new Directorate for State Threats and Cyber, as part of a concerted effort to increase significantly the resource the Home Office devotes to state threats, including Iran.

[371] Oral evidence – SIS, *** June 2023.

[372] Oral evidence – SIS, *** June 2023.

[373] Oral evidence – DI, *** June 2023.

- As of June 2023, the Middle East team within this new Directorate comprises *** FTE staff, who focus primarily but not exclusively on Iran. However, there are a number of further teams across HSG whose work is relevant to Iran but is "*thematically rather than geographically focussed*" (for example, broader counter-state threats strategy and legislation, cyber policy and border security).[374]

NSS

502. NSS told the Committee that it directs its resources "*holistically and in an actor-agnostic way, as represented in overall HMG strategies*".[375] Dedicated Iran resource apparently sits within the *** Middle East and Gulf team within NSS's International Affairs Unit. However, the Committee was not provided with any detail on this team, so we cannot provide assurance that NSS resourcing is proportionate to the threat and how the Iran response fares as part of the broader actor-agnostic approach.

Cross-Government capability

503. More broadly, we questioned how Iran-specific expertise is developed and maintained across Government. The External Experts we spoke to emphasised the importance of training Iran experts, and most voiced concerns that the Government lacked those with sufficient expertise. While Dr Vakil considered that, relatively speaking, "*the FCDO* [Foreign, Commonwealth and Development Office] *is far ahead of many governments in understanding the Iranian regime*",[376] our other External Experts considered strongly that much more needed to be done. Baroness Ashton told the Committee that she had been:

> *surprised at the lack of interest ... in talking to people who have actually engaged with Iran. The current Chief Negotiator, Bagheri, I spent two years with and I have said many times I would be very happy to brief those going out to meet him ... but there is not much interest.*[377]

The Committee was also told that "*in the two years I spent at the Foreign Office, there was one research analyst on Iran*" and that "*if you have people running policy in the Foreign Office who don't speak a word of Persian, then that is a fat lot of good, to be honest*" – a damning insight.[378]

504. While it appears that the Foreign Office may be in the process of building this expertise,[379] our External Experts expressed concern that it was not being prioritised: "*as you might imagine, the Treasury comes in and says we don't have any money. Well, it doesn't cost that much to train a Persianist, it takes time, but my point is that we used to be much, much more prepared for this sort of challenge*".[380] When we put this to the Foreign Secretary, he

[374] Written evidence – HMG, 27 October 2021.
[375] Written evidence – HMG, 27 October 2021.
[376] Oral evidence – Dr Sanam Vakil, 21 March 2023.
[377] Oral evidence – Baroness Ashton, 21 March 2023.
[378] Oral evidence – 2023.
[379] For example, in January 2024, the FCDO told the Committee that the Head of the Iran Unit was a Farsi speaker.
[380] Oral evidence – Professor Ali Ansari, 9 March 2023.

agreed that, "*when you talk about Farsi speakers, when you are talking about the kind of analysts that we need, you cannot turn on a sixpence*", but argued that his focus was on retaining existing Intelligence Community capability, given the additional costs required to train the requisite language and technical skills.[381]

505. Yet, one of the National Security Council (NSC) Iran Strategy campaigns, 'Enabling the Relationship', appears to focus on strengthening Iran expertise across HMG. When we asked the Deputy National Security Adviser (DNSA) what was being done – including on language skills and cultural understanding – he told the Committee that a programme existed, but then explained that this was actor-agnostic and focused on state threats generally as opposed to Iran specifically:

> *What we are trying to do from a broader countering state threats perspective is to really kind of grow that cadre of people that understand, you know, our approach but also how that pertains to all of the three kind of principal state threats ... to try and improve our understanding of state threats writ large.*[382]

It therefore appears that the Government is not building Iran capability: beyond mention in a Strategy campaign, nothing is actually being done to develop a future pipeline of Iran capability – despite the strong likelihood that the threat will increase in the coming years.

TTT. Resourcing on Iran has fluctuated over the past decade, supporting the concern that the response to the Iranian threat has been short-termist. * resourcing did not then increase following *** – given that Iran has consistently reduced its compliance since then.**

UUU. We have previously made reference to the fact that the Agencies do not have unlimited resources, and therefore hard choices on resourcing and prioritisation must be made during national security crises. It is clear to us that the situation during the conflict in Ukraine, for example, is no different.

VVV. GCHQ in particular recognises that its drawdown in resourcing * had significantly affected *** While GCHQ argued that it was doing 'more for less', this is nevertheless concerning.**

WWW. MI5 has still not been given the additional funding and resources that we called for in our *Extreme Right-Wing Terrorism* Report. Without a commensurate increase in resources, MI5 cannot be expected to absorb responsibility for an increased range of issues, without other areas of work suffering as a consequence.

XXX. Across Government, there is a lack of Iran-specific expertise and seemingly no interest in building a future pipeline of specialists, beyond mention in a Strategy campaign. We were particularly struck by the critique, "*if you have people running policy in the Foreign Office who don't speak a word of Persian, then that is a fat lot of good, to be honest*".

[381] Oral evidence – Foreign Secretary, 6 July 2023.

[382] Oral evidence – NSS, *** June 2023.

YYY. The Government's response to the Iranian threat appears to be wrapped up with state threats or the Middle East. This may be positive if it means that Iran will benefit from synergies with work to counter other – perhaps more prominent – state threats. However, the risk is that this instead results in a less tailored and therefore less effective response to the Iranian threat.

USING INTERNATIONAL PARTNERSHIPS

506. In considering the finite resources the Intelligence Community allocate to the Iran threat, it is important to factor in the 'force multiplier' effect of the UK's international partnerships. In our 2023 *International Partnerships* Report, we explained how critical these partnerships are. They enhance the ability of the intelligence Agencies, the wider Intelligence Community and the Government to make sense of, and act in, an increasingly complex world, allowing the UK to share with allies the burden of countering the most acute threats to our national interests, and providing access to intelligence sources and capabilities beyond the UK's reach.

Key partners

507. During this Inquiry, the Intelligence Community were clear that collaboration with international partners with regard to Iran is essential to address intelligence gaps (we consider coverage in the next chapter). The Agencies maintain particularly deep operational collaboration with their US *** counterparts: UK, US *** policy objectives and intelligence requirements are broadly aligned with regard to Iran, with the principal aims of preventing Iran from developing a nuclear weapon and holding Iran to account for its destabilising activity in the region.

508. The primary relationships between the UK Intelligence Community and their US *** partners are:

- for SIS: the US Central Intelligence Agency (CIA) ***;
- for GCHQ: the US National Security Agency (NSA) ***;
- for MI5: the CIA, US Federal Bureau of Investigation (FBI) ***; and
- for DI: the CIA, US Defense Intelligence Agency (DIA), US National Geospatial Agency (NGA) ***.

509. The Chief of SIS explained that the UK benefits from the scale of the US's *** efforts on Iran – in the case of the US, due to the greater scale of its national security community and ***: "*we get the advantages when they make significant* [investment] … *we will get the intelligence out of this partnership, and vice-versa*". He also noted the exceptionally high level of trust between the partners:

> *when faced with the challenge of ***, that is a conversation we can have around how we *** and that is highly sensitive, very intimate and we would probably only do that with the US ***.*[383]

[383] Oral evidence – SIS, *** June 2023.

510. GCHQ emphasised the "*unique insights*" into the Iranian threat they gain from their partners.[384] It described these partnerships as "*being more than the sum of the parts ... we wouldn't be able to have that same sense of scale or effectiveness if we tried to do it on our own*"[385] – as is illustrated by the fact that ***. In turn, GCHQ shares its specific strengths in ***, and collaborates on cyber security, ***.

511. For MI5, *** (although the terminology is no longer in use, it is notable that prior to 2022 MI5 talked about its 'Strategic Partners' ***). *** in evidence to our International Partnerships Inquiry in 2021, Director General MI5 had told the Committee that ***[386] ***.

Interdependence or over-reliance?

512. It is clear that these partnerships are extremely valuable. However, the Committee noted the Intelligence Community's references to the UK *** intelligence from the US ***.[387] The Foreign Secretary told us that "*our joint work with the US *** is absolutely invaluable*"[388] and more broadly HMG acknowledged that "*it is doubtful whether the value *** could be replicated*".[389]

513. We questioned whether the Intelligence Community were too dependent on the US *** and what would happen if it chose not to share intelligence with the UK in the future. The Chief of Defence Intelligence (CDI) told the Committee that "*on the assessment piece, we are very much *** working with all the partners mentioned in terms of the intel coming in*", particularly ***[390] – appearing to suggest that DI ***.

514. The Foreign Secretary was rather robust, however, telling the Committee that the UK had "*a very high-functioning domestic capability ... if we had to stand alone, we could*".[391] Similarly, GCHQ told the Committee:

> *we have sovereign capabilities, *** we have our sovereign ability to run Computer Network Exploitation operations and we could certainly continue.*[392]

Nevertheless, the Foreign Secretary felt it unlikely that the UK would need to stand alone:

> *in my experience, the relationships endure even through changes of political leadership and there has been ... a remarkable level of resilience and trust that runs in parallel to the political relationship ...* [although] *it doesn't give us a complete 100% safety net, which is why maintaining our inherent capability is key as well.*[393]

[384] Oral evidence – GCHQ, *** June 2023.
[385] Oral evidence – GCHQ, *** June 2023.
[386] Oral evidence (International Partnerships Inquiry) – MI5, *** June 2021.
[387] Written evidence – HMG, 21 April 2022.
[388] Oral evidence – Foreign Secretary, 6 July 2023.
[389] Written evidence – HMG, 21 April 2022.
[390] Oral evidence – DI, *** June 2023.
[391] Oral evidence – Foreign Secretary, 6 July 2023.
[392] Oral evidence – GCHQ, *** June 2023.
[393] Oral evidence – Foreign Secretary, 6 July 2023.

515. The Chief of SIS also emphasised to the Committee that it was not just the UK benefiting from the partnership: "*we are a full partner with the *** ... we are pulling our weight – more than*".[394] He was clear that the UK provided significant value to the US *** in return:

> *this is an interdependence to mutual benefit. It is not a kind of dependency of us on this. We play our full part ... The 'dependence' word is one I don't recognise. I think this is mutual interdependence between equal partners.*[395]

For example, CDI noted the value to partners of DI's expertise in analysing imagery: "*we are in many cases providing the analysis of the data that then goes up to the US system ****".[396] The JIO also told the Committee that "*on the assessment side, we are far from just taking what the Americans give us, we have a robust give-and-take … it is not a sort of big brother/small brother or big sibling/little sibling relationship*".[397]

Legal and policy parameters

516. As noted in our 2023 *International Partnerships* Report, it is clearly in the UK's national interest that the Agencies and DI work with foreign partners where they can provide intelligence that protects our national security; however, doing so can, if not managed correctly, risk compromising the UK's legal and ethical standards and damaging the reputation of the Agencies and DI. The Committee has previously published reports scrutinising what happens in such circumstances when the UK's values have been compromised.[398] The legal frameworks which govern the Intelligence Community's collaboration with international partners are therefore vital.

Legal frameworks

The Agencies and DI now have robust legal, policy and internal guidance frameworks in place to minimise the risk of any of their work with overseas partners compromising UK law and values. The UK's international and domestic law obligations are a critical component of the Agencies' work with international partners. The UK is bound by international law and is a State Party to the following international treaties:

- the International Covenant on Civil and Political Rights (ICCPR), which states that "*no person shall be subjected to torture or to cruel, inhuman treatment or punishment*";[399] it also prohibits arbitrary detention and provides safeguards for detained persons;

[394] Oral evidence – SIS, *** June 2023.

[395] Oral evidence – SIS, *** June 2023.

[396] Oral evidence – DI, *** June 2023.

[397] Oral evidence – JIO, *** June 2023.

[398] *Detainee Mistreatment and Rendition: 2001–2010*, HC 1113, June 2018; *Detainee Mistreatment and Rendition: Current Issues*, HC 1114, June 2018.

[399] International Covenant on Civil and Political Rights (New York, 19 December 1966), Treaty Series No.6 (1977), Cmnd 6702.

- the European Convention on Human Rights (ECHR), which states that "*no one shall be subjected to torture or to inhuman or degrading treatment or punishment*";[400] like the ICCPR, the ECHR also provides safeguards for liberty and security of the person;
- the UN Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;
- the 1949 Geneva Conventions, which require humane treatment of detainees and specifically prohibit torture, and cruel and degrading treatment in the context of international armed conflict; Article 3 Common to the four Geneva Conventions covers situations of non-international armed conflict such as civil wars and requires humane treatment for all persons in detention (including those held by non-state actors); the 'Common Article 3' specifically prohibits torture, cruel, humiliating and degrading treatment and unfair trial and, given that most armed conflicts today are non-international, Common Article 3 is of the upmost importance; and
- the Statute of the International Criminal Court, which includes as 'war crimes' torture, and inhuman and degrading treatment prohibited under the 1949 Geneva Conventions in the context of an armed conflict.

The UK is also bound by customary international law and, in the context of international partnerships, Article 16 of the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts is particularly relevant. The UK considers Article 16 to reflect customary international law, and responsibility is engaged where a State materially aids or assists another State in the commission of an internationally wrongful act, if it does so with intent and knowledge of the circumstances of that wrongful act and the act would be internationally wrongful if committed by that State.

One of the building blocks of the Agencies' international partnerships is the sharing of information. However, before sharing intelligence with foreign partners, the Agencies need to think about the type of information they intend to share and what action (if any) their foreign partner will take. Sometimes the Agencies and DI will simply provide intelligence to their foreign partners 'for information' or they may include other caveats to restrict the foreign partners' use of the intelligence. In many cases, the Agencies and DI will provide intelligence to a foreign partner with a specific request that action be taken – for example, 'tell us everything you know about person X' or 'please detain person Y'. There is also a risk that, even if the Agencies share intelligence for one purpose, the foreign partner will actually use that intelligence for an entirely different purpose. As such, there are different considerations in play depending on the scenario.

[400] Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights) (Rome, 4 November 1950), Treaty Series No.71 (1953), Cmd 8969. The ECHR is implemented domestically by the Human Rights Act 1998.

When the Agencies share data with foreign partners that has been obtained under a warrant issued under the Investigatory Powers Act 2016, they must ensure that the receiving (foreign) partner has applied 'safeguards' to such an extent the Agencies consider appropriate. These safeguards must *correspond* to those required by the Agencies under the IPA ('corresponding safeguards') for the retention and disclosure of such material.

The Agencies therefore require foreign partners to ensure that the material they receive is stored in a secure manner; they minimise the numbers of copies taken of the material and the numbers of people to whom the material is disclosed; and they ensure the destruction of the material once there are no longer relevant grounds for retaining it.

Foreign partners are also required to provide safeguards in relation to: (i) the examination of material such that the communications and other information of persons known to be in the British Islands are given adequate protection; and (ii) the handling of confidential material. Further, restrictions must be in force to prevent material obtained from interception from being used in legal proceedings.

517. These frameworks are applied to the Agencies' and DI's collaboration with partners on the Iran threat, and this is particularly relevant to the US ***, given the scale of collaboration. Across all of their work – whether Iran or otherwise – the Agencies told the Committee that they do not work with partners if:

- they judge that UK actions in doing so would be in breach of international law;
- ***;
- they judge that the outcome of the operation risks being detrimental to the shared policy objectives; or
- the operation is not consistent with UKIC's ethics and values.

518. HMG told the Committee that "*all Agency operations, and their support to international partners, are compliant with international law*".[401] HMG told the Committee that, where it does engage in a joint operation, UK 'red lines' are made clear at the planning stage to ensure that legal and policy boundaries are observed, and these are regularly reviewed as an operation develops.

519. When the Committee asked for an example of when the UK has declined to participate in a partner-led operation in relation to Iran on the basis that this would breach the Intelligence Community's policy or legal parameters, we were told that "*SIS does not have an immediate example to hand of this happening*".[402] The Chief of SIS told the Committee that partners "*have a very sophisticated and well-developed understanding of what we can and cannot do in working with them. They understand our legal requirements and therefore they tend not to*

[401] Written evidence – HMG, 21 April 2022.

[402] Written evidence – HMG, 13 July 2023.

push it, to be honest".[403] GCHQ provided the Committee with one example where it declined to participate *** operations conducted by a partner and had reiterated the legal and policy reasons as to why it was not willing to participate. However, GCHQ also told the Committee that, as US *** partners have a detailed understanding of the UK's policy and legal parameters, GCHQ is generally not asked to participate in any operations which might breach those.

520. US and *** will refrain from collaborating with the UK where they assess there to be a divergence between their intentions and these UK parameters – for example, where they might be seeking to take *** action ***. The US *** have *** given assurances that UK intelligence will not be used to enable their *** operations without explicit consent. In the event that it was found that a US *** had used UK intelligence outside the agreed parameters, an urgent review would be conducted and elements of operational collaboration with the agency or agencies responsible might be halted. The Agencies told the Committee that they have no evidence or indication that the US *** have deviated from their commitments.

521. Nevertheless, in order to avoid inadvertently sharing intelligence that might enable unlawful action, across all of their work – whether in relation to Iran or otherwise – the UK Intelligence Community maintain a regular dialogue with partners to understand their operational intent – for example, where they may intend to conduct operations that the Intelligence Community judge would be unlawful for the UK. Often, an area of divergence relates to the use of force. The UK legal and policy position is that the UK will make a material contribution to the use of force by a foreign partner only where: (i) it is satisfied that there is a legal basis for the use of force under international law, all other relevant legal risks have been considered and the force will be used in accordance with international law; and (ii) following Ministerial authorisation. As a result, the Agencies have previously refused to provide information directly relevant to ***.

522. Despite this close understanding of partners' intent, there have been instances when operational plans had not been shared ***, even where these had affected UK interests. As we noted in our *International Partnerships* Report, even in the case of the UK's closest partners, as with any strong partnership occasional differences in approach are unavoidable. For instance, we were told that the UK had not been informed of ***. We questioned whether this occurred regularly, and the Chief of SIS told the Committee that "*those types of operations are usually extremely well* ***". HMG further noted that it may not [even] be told about the operation subsequently, "***".[404]

523. This understanding of *** did not appear to be shared by the Foreign Secretary, however. He told the Committee that "*we expect to be, and are, informed in advance about operations ... where action may impact UK equities*"[405] – which the Committee considers would surely have applied in the case of ***. We asked whether the UK Intelligence Community had made representations to *** about the fact that they had not been told about ***. The Chief of SIS was resigned, noting: "***", but he did say that "*if we felt that such an operation endangered our assets, we would definitely take it up with them*".[406]

[403] Oral evidence – SIS, *** June 2023.

[404] Written evidence – HMG, 13 July 2023.

[405] Written evidence – Foreign Secretary, 25 July 2023.

[406] Oral evidence – SIS, *** June 2023.

524. When the Committee asked whether the UK had ever taken action without telling *** in advance, the Chief of SIS responded: "*I don't know the answer to that question*."[407] However, HMG subsequently advised us that there would be instances where the UK would pursue operations against Iran without informing ***, particularly if no *** equities were involved. Generally, however, this would not be the case as the Agencies work routinely to deconflict operations with partners ***.

525. In addition to the policy and legal parameters that govern joint working with the US ***, the Committee questioned whether collaboration was affected by differences in national governments' policy positions. SIS told the Committee that: "*The relationship between the agencies is mature enough that we will keep sharing, even when our policy positions are not aligned, and that is as true for *** ... and the Americans*".[408] For instance, we were told that the UK Intelligence Community share intelligence with *** and the US on Iran's ***, even where there is a risk that their governments will draw different policy conclusions to the UK.

****

526. ***

527. ***[409]

528. ***[410] ***[411]

****

529. ***[412] ***[413]

****

530. ***[414]

531. ***[415]

532. ***[416]

Intelligence diplomacy

533. A key aspect of HMG's work with partners is 'intelligence diplomacy', which we examined in our International Partnerships Inquiry. HMG defines 'intelligence diplomacy' as "*the use of intelligence information and relationships to influence international action*".

[407] Oral evidence – SIS, *** June 2023.
[408] Oral evidence – SIS, *** June 2023.
[409] Written evidence – HMG, 21 April 2022.
[410] Written evidence – HMG, 21 April 2022.
[411] Quarterly Report – SIS, January–March 2017.
[412] Written evidence – HMG, 21 April 2022.
[413] Oral evidence – SIS, *** June 2023.
[414] ***.
[415] Written evidence – HMG, 25 August 2023.
[416] Oral evidence – MI5, *** June 2023.

This activity sits at the nexus between traditional intelligence work and diplomacy, and ranges from using intelligence partnerships to build alliances or encourage action on a particular issue, to the maintenance of alternative diplomatic channels with governments or non-state actors with which it is considered impolitic to have overt diplomatic relations. Even though this work is not considered to be 'covert', it nonetheless remains secret (and indeed secrecy is often fundamental to its continued success).

534. Intelligence diplomacy is an important tool through which HMG seeks to build the credibility of the UK's understanding of Iran with relevant partners, and to ensure the continued awareness of threats posed to UK security and interests by Iran and its aligned groups. We were told that intelligence diplomacy is "*vital to ensuring that the UK's closest allies share our understanding of Iran's actions and strategy*".[417]

535. HMG told the Committee that it uses *** relationships in the region to deliver messages and gather a wide range of local actors' views. HMG gave the example of ***[418] ***.

536. The Committee was told that HMG facilitated an alternative channel *** HMG explained that such activity "*tends to be where two sides are stuck, they cannot appear for maybe domestic political reasons … to be talking to the enemy and we can provide a way of discreetly engaging the enemy*".[419]

537. HMG also told the Committee that it had an alternative channel with ***. This was described as a useful way of passing messages to ***, which have generally focused on "***".[420]

538. However, the Committee was told that any HMG interaction with *** on issues relating to Iran was "*history now … we keep the channels open to *** but they are message-passing, stabilisation, avoiding of miscalculation type channels*".[421] (*** do have declared intelligence representatives in the UK whom HMG meet and engage with on narrow areas of shared interest.)

539. As we previously noted in our *International Partnerships* Report, more broadly, by virtue of their often strong personal relationships with key figures in the security and intelligence establishments of many countries, as well as their relatively high profile and name recognition in the world of intelligence, the Agencies can sometimes 'open doors' for Ministers and senior officials to meet senior figures to whom access may be difficult to arrange through diplomatic channels. As the Foreign Secretary noted, the "*'brand' of SIS and the other Agencies is particularly strong and you can see that with the access we get to people*".[422]

[417] Written evidence – HMG, 27 October 2021.
[418] Oral evidence – ***, *** June 2023.
[419] Oral evidence – ***, *** June 2023.
[420] Oral evidence – ***, *** June 2023.
[421] Oral evidence – ***, *** June 2023.
[422] *International Partnerships*, HC 288, 5 December 2023.

540. Further examples of successful intelligence diplomacy against Iran are:

- ***
- Operation GINGER, covered in detail below.

Operation GINGER

***[423] ***

ZZZ. The Agencies' partnerships with the US * on the Iranian threat are of critical importance, and the *** countries operate with an exceptionally high level of trust.**

AAAA. The Agencies' close collaboration with the US and other international partners in relation to the Iran threat appears to be one of their greatest assets: it yields great value and lessens burdens. However, it also appears to be a potential vulnerability, in that if this arrangement were to cease, it is doubtful whether the Intelligence Community would be able to respond to the Iranian threat anywhere near as effectively.

BBBB. Most countries – even our closest allies – will operate under different legal and ethical constraints to the UK. However, to protect the UK we have no choice but to work with other countries. The framework under which our Agencies engage is therefore of the utmost importance. The evidence we have received reassures us that where HMG engages in a joint operation, UK 'red lines' are made clear to ensure that legal and policy boundaries are observed and that, wherever possible, appropriate due diligence is carried out to ensure that information is not obtained via prohibited methods. However, we note that that cannot be guaranteed.

CCCC. We recognise the benefits of sharing intelligence *. The Community have taken steps ***.**

[423] Oral evidence – ***, *** June 2023.

UK INTELLIGENCE COVERAGE

541. In terms of gathering intelligence on Iran, witnesses emphasised that Iran is a hard intelligence challenge. The Intelligence Community told the Committee that their access to Iran is ***. The JIO told the Committee that the UK's intelligence coverage is "***" and that there are clear areas where the UK's coverage and understanding are ***.[424] We explore below the challenges of operating against Iran – and what this means in terms of the confidence the Intelligence Community have in their assessments and where they have the most and least coverage.

Operating against Iran

542. The Iranian regime's extensive domestic monitoring system is designed for internal repression. When we questioned the Intelligence Community as to whether it could also be used by the Iranian Intelligence Services (IIS) as an effective counter-espionage tool, they told us:

> ***.[425]

The Iranian government is highly sensitised to the threat of foreign intelligence work against it, and the penalties for those convicted of espionage are severe – including the death penalty.

543. HMG told the Committee that the Iranians' counter-espionage capability ***. The Chief of SIS said: "*Despite sanctions and the financially straitened circumstances of the country, their agencies remain well-resourced and therefore able to* ***". He described ***. SIS continued to ***: "*they* [the regime] *have pretty tight control over their own country* ... ***".[426] Covid-19 had further exacerbated the challenge ***.

544. The Committee asked the Intelligence Community about their ability to gather human intelligence on Iran. The Intelligence Community told the Committee that ***.[427]

545. To stay ahead of Iran's *** counter-espionage capabilities (which have been reported to include surveillance, biometrics and data aggregation[428]), the Chief of SIS told the Committee that "*we have to find cleverer and cleverer ways of using technology ourselves and the tradecraft that goes along with it ***. And that is a bit of an arms race*".[429] SIS told the Committee that it was working not to "*sleepwalk*" into a situation where technological developments ***.[430]

[424] Oral evidence – JIO, *** June 2023.
[425] Written evidence – HMG, 27 October 2021.
[426] Oral evidence – SIS, *** June 2023.
[427] Oral evidence – SIS, *** June 2023.
[428] 'The AI Assault on Women: What Iran's Tech-enabled Morality Laws Indicate for Women's Rights Movements', Council on Foreign Relations, 7 December 2023.
[429] Oral evidence – SIS, *** June 2023.
[430] Oral evidence – SIS, *** June 2023.

546. ***[431] ***[432] ***.[433]

547. In terms of GCHQ's coverage of Iran, the Committee was told that GCHQ uses *** of signals intelligence (SIGINT) and cyber capabilities, including ***. However, it faced similar challenges in terms of the Iranians' counter-espionage operations:

> *the fragility can be caused by the dynamism in the environment but Iran does have active counter-espionage capabilities and ***, so we have to be very cautious and aware of that.*[434]

548. GCHQ told the Committee that one of its primary focuses was to continue innovating and developing new technology, and refining its approach to SIGINT and cyber activity, to stay ahead of its adversaries. GCHQ considered that its "*investment in digital technology and digital transformation will enable us to continue to innovate and outpace our adversaries in that way*".[435]

549. The Committee asked the Intelligence Community about their ability to penetrate the IIS. ***, telling the Committee that: "***".[436] *** agreed, adding that:

> ***.[437]

Intelligence gaps and assessment confidence

GCHQ and SIS delivery against intelligence requirements

550. We detailed the intelligence requirements that GCHQ and SIS were set by the Intelligence Outcomes Prioritisation (IOP) Plan in 2021 earlier, in the 'Strategy and Policy Response' chapter.

551. In 2021, we were told that GCHQ's effort on the IOP Plan requirements was spread equally between ***, with a smaller effort on ***. We were later informed that, of the IOP Plan requirements GCHQ had been set, it was meeting expectations on approximately one-third (***) and partially meeting expectations on approximately two-thirds (***). (We were not provided with a more detailed breakdown than this.) The Committee was told that, whilst *** is the primary reason for the IOPs only partially being met, this should be considered in combination with Iran being a hard intelligence target.

552. In terms of SIS, the Committee was told that its effort in 2021 had been "*balanced across ****".[438] In 2023, SIS did not provide a full breakdown of how many requirements it

[431] Written evidence – SIS, 16 January 2023.
[432] Written evidence – SIS, 16 January 2023.
[433] Oral evidence – SIS, *** June 2023.
[434] Oral evidence – GCHQ, *** June 2023.
[435] Oral evidence – GCHQ, *** June 2023.
[436] Oral evidence – ***, *** June 2023.
[437] Oral evidence – ***, *** June 2023.
[438] Written evidence – HMG, 27 October 2021.

had 'met' or 'partially met'. However, SIS did tell the Committee that it had 'met' expectations of its requirements relating to ***, but had only 'partially met' expectations in relation to Iranian ***.

DI coverage and analysis

553. As covered in the 'Strategy and Policy' chapter, DI is tasked through the Defence Strategic Intelligence Prioritisation Process. The Chief of Defence Intelligence (CDI) told the Committee that, on Iran, DI's intelligence collection and analysis activities (as distinct from its all-source assessments) are focused primarily on:

- GEOINT (geospatial intelligence) – such intelligence might generally be used to detect, for example, *** ballistic missiles or the development of missile testing sites. DI told the Committee that it has ***;
- MASINT (measurement and signals intelligence) – CDI noted ***;
- HUMINT (human intelligence) – we were told that ***; and
- OSINT (open source intelligence) – DI's efforts in this area have expanded as the amount of open source material has grown and as the technologies used to interpret open source material have developed. DI's analysis of open source information particularly focuses on "***".

554. CDI told us that DI's coverage *** the above areas allow it to develop "*good insights into* [Iran's] *overall posture*",[439] including indicators and warnings for regional escalation.

Intelligence gaps

Assessment probability and confidence

The JIO and the wider UK intelligence assessment community use a 'probability yardstick', which states how likely something is:

- Up to 5% (i.e. a 1 in 20 chance) is a 'remote' chance.
- 10–20% (between 1 in 10 and 1 in 5) is 'highly unlikely'.
- 25–35% (1 in 4 to 1 in 3) is 'unlikely'.
- 40–50% (2 in 5 to 1 in 2) is a 'realistic possibility'.
- 55–75% (5 in 9 to 3 in 4) is 'likely or probable'.
- 80–90% (4 in 5 or 9 in 10) is 'highly likely'.
- 95–100% (19 in 20 or more) is 'almost certain'.

[439] Oral evidence – DI, *** June 2023.

The JIO and other assessment bodies also use confidence statements to indicate the extent to which their judgements are informed by evidence:

- 'Low' confidence means that judgements are based on fragmentary, ambiguous and/or contradictory source material.
- 'Medium' or 'Moderate' confidence judgements will have elements of corroboration, based on quality material but have key gaps, concerns or weaknesses.
- 'High' confidence means that judgements are based on a range of good-quality sources, potentially with some corroboration.

555. It is clear that changes in the context, such as the death of General Qasem Soleimani and consequent internal changes could create challenges. In terms of confidence, the JIO told us that across Iran-related issues, its degree of confidence varied by subject. Overall, it had *** confidence, which has been *** over time.

556. The Intelligence Community told the Committee that broadly speaking, their coverage on Iran was "***". The Intelligence Community admitted that there was "***", and it appeared from the evidence we received that there were some intelligence gaps. In terms of the cyber threat, the complexity of the cyber landscape means that there may never be complete coverage. When we requested further information on the specific areas of greatest and least coverage and particular intelligence gaps, the Intelligence Community responded that such information would "*only provide a snapshot accurate at the moment of its recording*".[440]

557. Nevertheless, we questioned how intelligence coverage on Iran compared with that on China and Russia – similarly hard targets. The Intelligence Community said that – from a *** all three are "*very difficult, hard targets for a variety of reasons*".[441]

558. The Intelligence Community noted the particular challenges presented by the specific nature of the Iranian regime:

> *you have the theocrats at the top and then you have ... the different bits of the security architecture and the civilians and the MFA* [Iranian Ministry of Foreign Affairs] *all, sort of, fighting amongst themselves ... the Iranian regime and system is not as organised ... as the Chinese and Russians ... because of that sort of Balkanised fragmented nature, ***.*[442]

[440] Written evidence – HMG, 21 April 2022.

[441] Oral evidence – ***, *** June 2023.

[442] Oral evidence – JIO, *** June 2023.

559. Director General MI5 noted that:

> *elements of what happens in Iran are a bit more unpredictable typically on average than some of what happens inside Moscow or Beijing.*[443]

Diplomatic coverage

560. When we questioned how coverage on Iran compared with that on China and Russia, the JIO told us that, broadly speaking, the lack of a consistent diplomatic presence in Tehran meant that the depth of the UK's understanding from diplomatic reporting was less than on Russia and China (where the diplomatic presence has been more constant).

Iranian intent

561. From the evidence we considered, it appeared that the Intelligence Community have a *** understanding of Iranian capability, and *** understanding of Iranian intent. GCHQ described its understanding of *** as "***"[444] and, as the Threat section of this Report noted, there *** (for example, ***). To a certain extent, *** which JIO described as ***.

562. The JIO highlighted Iran's intent to weaponise its nuclear programme as an area in which they had *** confidence, which had *** in recent years, as a result of ***:

> *On Iranian intent we are at *** confidence because ***.*[445]

563. ***[446] ***[447] ***.

564. An example of the practical impact of the uncertainty around *** was provided by DI – it told the Committee that the intelligence gaps around *** taken together meant that the possibility of a fundamental misunderstanding *** "*could lead to war*".[448]

Operational plans

565. For MI5, a particular challenge *** was ***:

> *So we have a pretty good level of understanding of ***. We know quite a bit about ***, that is the bit that is always hard for us to unearth.*[449]

DDDD. Iran is a hard intelligence target, comparable to Russia and China. The regime appears to be highly sensitised to the threat of foreign intelligence work against it (the Committee noted in particular the regime's domestic monitoring system, *). The Intelligence Community's access to Iran is ***.**

[443] Oral evidence – MI5, *** June 2023.
[444] Oral evidence – GCHQ, *** June 2023.
[445] Oral evidence – JIO, *** June 2023.
[446] Oral evidence – GCHQ, *** June 2023.
[447] Written evidence – HMG, 13 July 2023.
[448] Oral evidence – DI, *** June 2023.
[449] Oral evidence – MI5, *** June 2023.

EEEE. While SIS continues to *, the tight control the regime exercises ***.**

FFFF. Overall, the Intelligence Community have * coverage of Iran's capability, *** understanding of its intent, particularly in relation to Iran's ***. Given the potential for misunderstanding and miscalculation between Iran and Israel, this is of the utmost concern.**

DEFENDING THE UK

566. As explored already, the threat posed by Iran in the UK has grown in recent years. The Home Secretary told us that the UK was monitoring the threat closely and responding with "*heightened awareness ... heightened prioritisation and heightened resource to match it*". She also told the Committee that: "*anticipating an escalation is the prudent approach*".[450]

567. In this chapter, we consider the broad responsibilities of the Home Office, MI5 and the National Cyber Security Centre in respect of defending the UK from the Iranian threat, before going on to consider in the following chapters the Government response to each of the elements of the threat to the UK: the threat of a physical attack on individuals, the espionage threat, offensive cyber, interference, the nuclear programme, and the threat to UK interests in the Middle East.

Responsibilities

Home Office

568. We referred, in the 'Ministerial Responsibilities' chapter, to the Home Office's policy responsibilities relating to Iran, which include: the domestic response to state threats (including the development of new legislation); policy on investigatory powers; preventing terrorism; and tackling cyber-crime. This is in addition to the Home Office's delivery responsibilities, including the use of legislative tools such as proscription and the operation of the National Security Act 2023 regime.

569. The Home Office and Foreign, Commonwealth and Development Office (FCDO) jointly lead work on countering Iranian state threats to the UK (***). The objectives of this work include countering Iran's intent and ability to cause harm to people in the UK or to British people and assets overseas – and part of this is achieved through work "*to increase the hardening of the environment here to make it harder for them to operate*".[451]

570. The Home Office also leads the 'Protect' strand of the Counter-State Threats Strategy (CSTS). As addressed in the 'Strategy and Policy Response' chapter, it was not clear how the CSTS linked to the National Security Council (NSC) Iran Strategy, and it is therefore unclear how the 'Protect' strand of the CSTS aligns with the 'Threats to the UK' pillar of the NSC Iran Strategy. However, as the Home Office leads on both, the Committee presumes that it has taken steps to ensure that synergies are taken advantage of and duplication is eliminated.

571. HSG established a new Directorate for State Threats and Cyber in September 2021; however, as detailed in the 'Resourcing' chapter, as of June 2023 the Middle East team in that directorate comprises just *** staff. It is unclear how much Iran features in the broader,

[450] Oral evidence – Home Secretary, 6 July 2023.

[451] HSG Quarterly Report, January–May 2021.

actor-agnostic work of its thematic teams (such as those looking at state threats, cyber policy and border security) – and whether it is eclipsed by the state threats posed by Russia and China.[452]

MI5

572. Under the Security Service Act 1989, MI5 is responsible for countering state threats, i.e. "*protection against threats from espionage, terrorism and sabotage* [and] *from the activities of agents of foreign powers*". MI5's Counter State Threats mission primarily focuses on Iran, Russia and China but also has a 'Rest of the World' remit. As addressed in the 'Resourcing' chapter, in 2021 MI5 had *** full-time equivalent (FTE) staff working in its Counter State Threats mission, and, in September 2021, *** of those staff were dedicated to Iran specifically.[453]

573. MI5 told the Committee that some of the factors it needed to consider in terms of its counter-espionage operations to tackle Iranian Intelligence Services (IIS) activity in the UK were:

- <u>scale of activity</u>: ***;
- <u>persistence of the threat</u>: ***; and
- <u>breadth of the threat</u>: as covered in the Threat section of this Report, the IIS present a multi-faceted threat to the UK, requiring a similarly broad MI5 response.

574. MI5 told the Committee that, given the breadth of the Iranian threat and MI5's finite resources:

> ***.[454]

When we questioned what exactly that might entail, MI5 told the Committee:

> ***.[455]

575. As covered in the Committee's *Russia* and *China* Reports, HMG uses a variety of tools to disrupt hostile activity by state threat actors, including Iran. These tools include the following:

- **Interviews:** *** may arrange a discussion with that individual, with the aim of ***.
- **Vetting action:** Removing the security clearance of British nationals with access to sensitive information who pose a national security risk, including those who may have been in contact with foreign intelligence services.

[452] Although, later in this Report, we explore the work of the Home Office and its use of immigration tools.

[453] As previously noted in the 'Resourcing' chapter, staff working in the Iran Mission also have access to the resource of specialist covert intelligence collection teams, which provide, for example, surveillance or technical capability, and to a range of analysts and assessment capability.

[454] Written evidence – HMG, 27 October 2021.

[455] Oral evidence – MI5, *** June 2023.

- **Expulsion of intelligence officers:** Removal of intelligence officers operating in the UK under diplomatic cover (under the terms of the Vienna Convention).
- **Visa action:** As is standard, the Home Office can consider revoking a visa on the grounds that someone's presence in the UK is not conducive to the public good. *** For example, *** visa was revoked for ***
- **Démarches:** This might include, amongst other things, requesting the removal of named intelligence officers from their positions ***
- **Briefings to industry:** These are used where intelligence indicates there is intent to target certain companies or industry sectors by state threat actors. This work is led by NPSA[456] (formerly CPNI[457]) and National Cyber Security Centre.

When the Committee questioned which of these tools were of most use in the case of Iran, the Director General MI5 said: "*the entire operational toolkit ... is in play when it comes to Iran*".[458]

576. MI5 also has responsibility for the Joint State Threats Assessment Team (JSTAT). JSTAT provides assessments and a holistic view on the national security threat posed by:

- espionage;
- assassination;
- interference in UK democracy and society;
- threats to the UK's economic security; and
- threats to the UK's people and assets overseas.

JSTAT has had *** on ***[459] *** the Committee was told that JSTAT anticipated that its Iran-related work would grow ***.

National Cyber Security Centre

577. The National Cyber Security Centre (NCSC), part of GCHQ, is the UK's technical authority on cyber security, and works closely with law enforcement agencies, the Intelligence Community and the cyber security industry, in order to prevent, disrupt and investigate cyber-related threats, including from Iran. GCHQ told us that "*cyber threats from Iran have been a feature and a priority for the NCSC since inception and for many organisations as well*".[460]

578. NCSC gathers intelligence on the Iranian cyber threat, developing knowledge of intent, capabilities and individuals involved, enabling attributions and disruptions that are intended to deter further harmful activity. NCSC works closely with industry, with which it exchanges information on the cyber threat in real time.

[456] National Protective Security Authority.

[457] Centre for the Protection of National Infrastructure.

[458] Oral evidence – MI5, *** June 2023.

[459] Written evidence – HMG, 27 October 2021.

[460] Oral evidence – GCHQ, *** June 2023.

LEGISLATION, SANCTIONS AND PROSCRIPTION

579. The Committee noted in its China Inquiry that, while the Government did not have the right tools to tackle the hostile state threat, one of the tools that could be developed and used quickly is legislation. Until recently, the Official Secrets Acts[461] were the only pieces of UK legislation which specifically addressed state threat activity.[462] However, during the time covered by this Inquiry, the National Security Act 2023 completed its passage through Parliament. We consider this new legislation to be a step in the right direction, although we will need to see how effective it is at addressing the Iranian threat specifically.

580. In terms of Iran, sanctions are a more well-established tool. The UN passed multiple Security Council Resolutions between 2006 and 2010 – including sanctions measures – against Iran, mainly focused on its nuclear programme, and the UK makes frequent use of sanctions as a tool against the Iranian regime – for example, in response to the recent protests in Iran.

581. Proscription is another tool which the Government has at its disposal, and which has already been used in respect of several Iran-supported groups assessed to be concerned in terrorism, such as Lebanese Hizbollah and Hamas – but not yet the Islamic Revolutionary Guard Corps (IRGC).

Legislation

The Official Secrets Acts regime

582. The Official Secrets Acts 1911, 1920 and 1939 set out offences relating to espionage and were designed to combat state threats.[463] However, in the course of our Inquiries into national security issues relating to China and Russia, it became clear that these legislative measures were inadequate in countering state threat activity. For instance, under the Official Secrets Acts regime, it was not an offence to be a covert agent of a foreign power. The Committee's *Russia* Report concluded that "*it is very clear that the Official Secrets Act regime is not fit for purpose ... It is essential that there is a clear commitment to bring forward new legislation to replace it ... that can be used by MI5 to defend the UK against agents of a foreign power*."[464] During this Inquiry, we were told that the Intelligence Community had historically found it challenging tackling malign foreign influence in the UK, as previously much of this activity fell "*within the 'legal but harmful' threshold*".[465]

583. In the December 2019 Queen's Speech, the Government confirmed plans to introduce a new Espionage Act to provide a legislative framework to deal with Hostile State Activity (which has since been referred to as 'State Threat Activity' or 'State Threats', to avoid 'hostile' being interpreted as qualifying 'state' rather than 'activity'). In September 2020,

[461] 1911, 1920 and 1939.
[462] Other than the 'ports stop' power introduced in the Counter-Terrorism and Border Security Act 2019.
[463] The Official Secrets Act 1989 sets out offences relating to the unauthorised disclosures of certain categories of sensitive information.
[464] *Russia*, HC 632, 21 July 2020.
[465] Written evidence – HMG, 25 August 2023.

HMG confirmed that the Home Office was working on legislation to create a Foreign Agents Registration Scheme and reform the Official Secrets Acts. The Committee had called for such a scheme for many years, as had the Law Commission (which found that the espionage offences in the Official Secrets Acts 1911–1939 were "*very wide but rarely prosecuted*" as a result of dated and obscure drafting and complex supporting case law).[466]

The National Security Act 2023

584. The National Security Bill was introduced in Parliament on 11 May 2022, and the Act received Royal Assent on 11 July 2023. The Act modernises the Official Secrets Acts' 'espionage' regime and creates new offences, such as sabotage, foreign interference and assisting a foreign intelligence service. HSG told the Committee that this legislation and the powers it creates will strengthen HMG's ability to counter the threat posed by Iran: "*we will have a much stronger range of legislative tools for the Agencies and the police to help us bear down on the threat*".[467]

585. MI5 also told us that the Act would strengthen its ability to counter state threats and that it was "*very optimistic*" that it would support its Iran-related work and address some of the legislative gaps that it has seen most frequently:

> *in particular the new offence of assisting a foreign intelligence service. Quite often Iranian activity is reasonably sophisticated and we don't always *** the ability ultimately to bring a prosecution ... So we don't necessarily want to wait for a conspiracy to murder to be made out in, quote, 'usable evidence', but if we can, as it were, earlier in the gestation of some activity prove that an individual is wittingly assisting the Iranian Intelligence Services, that would feel to us like a potentially quite impactful new power.*[468]

586. As well as reforming the Official Secrets Acts, the National Security Act 2023 created a Foreign Influence Registration Scheme (FIRS), which was a key recommendation of the Committee's *Russia* Report. The establishment of the FIRS will help UK law enforcement and the Intelligence Community to tackle the complex and varied threats posed by state threat actors. It will increase the transparency of those threats and help to make the UK a more difficult operating environment for foreign intelligence services. This should help to deter state threat actors from undertaking harmful activity and, where such activity is undertaken, disrupt it at a much earlier stage.

587. The FIRS operates as a two-tier system – the Political Influence Tier and the Enhanced Tier. The Political Influence Tier requires the registration of arrangements to carry out political influence activities in the UK at the direction of a foreign power. The Enhanced Tier builds on this, by giving the Home Secretary the power to require registration of a broader range of activities for specified countries, parts of countries or foreign government-controlled entities, where this is necessary to protect UK interests.

[466] *Protection of Official Data Report*, Law Commission, HC 716, September 2020.
[467] Oral evidence – HSG, 21 June 2023.
[468] Oral evidence – MI5, *** June 2023.

588. The Home Office told the Committee that "*Iran will be considered for the Enhanced Tier of FIRS once the scheme is operational*",[469] and MI5 told the Committee that, "*if Iran were to be designated under that power, that would come at some of the activity that we have been describing* ***".[470] The Home Secretary did not say whether Iran would be designated under the Enhanced Tier: "*It would all depend on the particular facts and circumstances of the entity to be registered but I would not rule it out at all*".[471] The Committee recognises that this decision will require proper consideration, nevertheless we would be surprised if Iran were not deemed worthy of inclusion under the Enhanced Tier – if it were not, it is hard to see which countries would be.

589. However, the National Security Act 2023 reformed only the Official Secrets Acts' 'espionage' regime; it did not reform the Official Secrets Act 1989 – as recommended by the Committee, and separately by the Law Commission in its 2020 report *Protection of Official Data*. This is disappointing, given that the Government's 2021 public consultation had given a commitment that "*the legislative proposals being developed by the Government will therefore include, at a minimum ... reform of the Official Secrets Act 1989*".[472] This fundamental omission means that the current problems with the Official Secrets Act 1989 – which have already been acknowledged by the Government – will persist. These problems include the requirement to prove damage for unauthorised disclosures[473] – which acts as a significant barrier to prosecutions – and the two-year maximum sentence, which is insufficient to deter or respond to the most serious unauthorised disclosures.

590. During Second Reading of the National Security Bill in the House of Commons, Members of the Committee therefore sought assurances that reform of the Official Secrets Act 1989 would be brought forward with "*some urgency*". Although the Government did not commit to a timeline, the then Home Secretary clearly stated that "*I can assure the House that as soon as we can, when we find the right moment, we will come back to this*".[474] We therefore understood that the Government still intended to bring forward reforms.

591. During this Inquiry, the Director General of HSG told the Committee that she "*certainly expect*[ed] *there to be much more frequent legislation on state threats in the coming years than there has been ... as we tighten up, clearly our adversaries will respond and will look*

[469] Written evidence – HMG, 13 July 2023.

[470] Oral evidence – MI5, *** June 2023.

[471] Oral evidence – Home Secretary, 6 July 2023.

[472] Legislation to Counter State Threats (Hostile State Activity), Government Consultation, Home Office, 13 May 2021.

[473] The Official Secrets Act 1989 created offences associated with the unauthorised disclosure of information in the following categories: security and intelligence; defence; international relations; crime and special investigation powers; information relating from authorised disclosures entrusted in confidence; and information entrusted in confidence to or by other states or international organisations. In creating offences under these categories, the Act distinguishes between current and former employees of the security and intelligence services, and crown servants (for example, Ministers, civil servants, members of the police and Armed Forces) or Government contractors. Provisions relating to members of the security and intelligence services stipulate that any unauthorised disclosure relating to security and intelligence is an offence. On the other hand, for crown servants and Government contractors, the Act stipulates that they can only be found guilty of an offence if the unauthorised disclosure is deemed 'damaging' ('Official Secrets Act 1989: Disclosure of Official Information', House of Lords Library Briefing, 18 April 2019).

[474] National Security Bill, Second Reading, *Hansard*, 6 June 2022.

for additional gaps that we will then look to plug. So we will be in, to an extent, a legislative arms race with our state adversaries for the coming years".[475] However, in relation to Official Secrets Acts reform specifically, we were told: "*we very much heard the concerns around OSA 89* [Official Secrets Act 1989] *as the National Security Bill went through, including from this Committee ... it is something that we will continue to look at ...* [we are] *committed to continuing to look at it*".[476] When we then pushed the Home Secretary as to when that might be, she gave quite a different answer: "*We don't repeal the 1989 Act. It is something that we haven't, we don't have plans to do ... we haven't identified a need to go further, as of yet*".[477] This discrepancy appears to represent a worrying change in the Government's position, given the assurances previously given to this Committee and to Parliament.

Computer Misuse Act 1990

592. In February 2023, the Security Minister launched a Call for Information[478] as part of a review of the Computer Misuse Act 1990, which HSG described as necessary "*to ensure that* [the Act] *remains able to tackle the ever-changing cyber threat*"[479] – which appears particularly relevant in the context of the aforementioned cyber threat from Iran. The Call for Information ran until April 2023, and sought views from law enforcement agencies, domain name registrars and hosting providers on three proposals in particular:

(i) the creation of a new power to allow law enforcement agencies to take control of domains and Internet Protocol (IP) addresses where these are being used by criminals to support a wide range of criminality;

(ii) the creation of a new power to allow a law enforcement agency to require the preservation of computer data in order to allow that agency to determine whether the data would be needed in an investigation (the power would not allow the agency to seize the data); and

(iii) the creation of a new power to allow action to be taken against a person possessing or using data obtained by another person through an offence under the Computer Misuse Act (subject to appropriate safeguards being in place).

593. During our Inquiry, the Home Office told the Committee that "*Home Office officials are now working with the private and public sector on their feedback, including specific measures which would improve the UK's ability to tackle cyber-crime*".[480] However, as at October 2023, we had still not been provided with an update.

[475] Oral evidence – HSG, 21 June 2023.
[476] Oral evidence – HSG, 6 July 2023.
[477] Oral evidence – Home Secretary, 6 July 2023.
[478] A public consultation to seek views on a policy or legislative change proposed by the Government.
[479] HSG Quarterly Report, January–May 2021.
[480] Written evidence – HMG, 25 August 2023.

Sanctions

What are sanctions?

The UK Government defines sanctions as:[481]

> *restrictive measures that can be put into place to fulfil a range of purposes. In the UK, these include complying with UN and other international obligations, supporting foreign policy and national security objectives, as well as maintaining international peace and security, and preventing terrorism.*

The UK imposes sanctions on states, groups or individuals, and they include:

- trade sanctions, including arms embargoes and other trade restrictions;
- financial sanctions, including asset freezes;
- immigration sanctions, known as travel bans; and
- aircraft and shipping sanctions, including de-registering or controlling the movement of aircraft and ships.

As sanctions can be co-ordinated with allies, this allows the UK to maximise the impact they have when seeking to dissuade groups from pursuing particular goals.

594. The UN passed multiple Security Council Resolutions to impose sanctions on Iran between 2006 and 2010, focused on its nuclear programme. These sanctions were an important factor in bringing Iran to the negotiating table, culminating in 2015 in the Joint Comprehensive Plan of Action (JCPOA), which exchanged sanctions relief for restrictions on Iran's nuclear programme. However, in May 2018, the then US President Trump announced the US's reimposition of sanctions on Iran, citing concerns that Iran's destabilising regional activity – including its development of ballistic missiles – was not addressed in the JCPOA.

595. Independent of the UN sanctions relating to Iran's nuclear programme, the UK has also imposed sanctions on Iran for other violations. For example, in response to the recent protests in Iran, the UK has used sanctions to add pressure on the regime. The UK's response has been largely co-ordinated with the EU and US – for instance, the UK joined the EU and US in sanctioning Iran's morality police in October 2022, and Iranian officials in November 2022 and January 2023. The UK also introduced additional sanctions on Iran's Prosecutor-General in response to the execution of British-Iranian dual national Alireza Akbari.

[481] 'Guidance: UK Sanctions', FCDO, 24 February 2022.

UK sanctions against Iran

596. As at January 2023, the UK has imposed financial sanctions on 508 individuals and 1,189 entities relating to Iran. The majority of these are companies involved with the nuclear programme but they also include sanctions for human rights issues. The Foreign Secretary told us that the Foreign, Commonwealth and Development Office (FCDO) had "*taken specific sanctions action in response to state threat activity and with regard to the other priorities, including the brutalisation of Iranians by the regime itself*".[482] The Deputy National Security Adviser (DNSA) expanded further:

> *there has been a swathe of sanctions that have been taken forward in the last period, 10 sanctions packages, for example, targeting over 300 Iranian individuals and entities in response to human rights violations, terrorism, proliferation of weapons ... those will be targeted at IRGC members or members of militia, the judiciary and security services.*[483]

597. The FCDO is responsible for the sanctions process. Designation cases are developed by a team *** which monitors relevant intelligence and regularly consults the Intelligence Community. The Foreign Secretary told the Committee that intelligence had contributed to the enforcement of sanctions against Iran, including on:

- enabling work against Iranian-owned or aligned ***;
- supporting sanctions against specific *** entities;
- enabling the UK to avoid inadvertently breaking sanctions;
- ***

An effective tool?

598. Our External Experts were not convinced that sanctions are effective in encouraging Iran to change its behaviour. They were critical of a strategy to "*sanction Iran into obedience ...* [when] *all it does is encourage disobedience ... the consistent overestimate by countries like the United States that sanctions would 'bring Iran to heel' has been disproved*".[484] They also noted that, whilst US sanctions had a significant negative impact on Iran's economy, the International Monetary Fund (IMF) had still projected economic growth for Iran of 2% in 2023 – and there was also a risk that Iran would respond to Western sanctions by deepening its economic relationship with China.

599. We asked the Intelligence Community whether they considered that sanctions would deliver behavioural change, or drive Iran further towards other state threat actors. The DNSA told the Committee that the National Security Council (NSC) did consider "*secondary consequences*" when determining the UK's overall policy approach towards Iran.[485] However,

[482] Oral evidence – Foreign Secretary, 6 July 2023.
[483] Oral evidence – NSS, *** June 2023.
[484] Oral evidence – Sir Richard Dalton, 9 March 2023.
[485] Oral evidence – NSS, *** June 2023.

it was unclear whether this related to sanctions specifically, and whether the NSC had considered – in the limited time it had devoted to discussions on Iran – in particular whether sanctions would be effective in encouraging behavioural change.

Proscription

600. The Home Secretary has the power to proscribe an organisation under the Terrorism Act 2000. Proscription is the banning of an organisation based upon a reasonable belief that it:

- commits or participates in terrorism;
- prepares for terrorism;
- promotes or encourages terrorism (including the unlawful glorification of terrorism); or
- is otherwise concerned in terrorism.

In considering whether to exercise their discretion to proscribe an organisation, the Home Secretary will take into account other factors, including:

- the nature and scale of an organisation's activities;
- the specific threat that it poses to the UK;
- the specific threat that it poses to British nationals overseas;
- the extent of the organisation's presence in the UK; and
- the need to support other members of the international community in the global fight against terrorism.

If an organisation is proscribed, it is illegal in the UK to belong to that organisation or to invite support for that organisation, with a maximum penalty of 14 years' imprisonment and/or a fine.

Islamic Revolutionary Guard Corps proscription

601. The Home Office has proscribed several groups assessed to be concerned in terrorism which have a relationship with (and to varying degrees receive support from) Iran, such as Al-Qaeda, Hamas and Lebanese Hizbollah. While IRGC members and activities have been targeted by UK sanctions,[486] the IRGC as an organisation has not been proscribed under the Terrorism Act. There have, however, been calls for the UK to proscribe the IRGC as a terrorist organisation, particularly in response to recent actions attributed to the IRGC. These actions include a terror attack against a German synagogue in November 2022, and repeated assassination attempts within the UK throughout 2022. His Majesty's Opposition stated its support for proscribing the IRGC after the execution of British-Iranian national Alireza Akbari in January 2023.

[486] A full list of those sanctioned can be found at: 'Financial Sanctions, Iran (Human Rights)', GOV.UK, 15 September 2023.

602. Media reporting in January 2023 suggested that the Government would announce within weeks that it would be proscribing the IRGC; however, by February, further reporting suggested that this had stalled because the FCDO wished to prioritise maintaining communication channels with the regime. The Foreign Secretary emphasised the diplomatic implications of such a decision, telling the Committee that "*no course of action is completely cost-free … limiting my* [toolbox] … *is something that I would take ... seriously*".[487] However, we note that – as previously mentioned – the Foreign Secretary has not invested in building a relationship with his Iranian counterpart, so we question whether a decision to proscribe the IRGC could possibly have any impact in that respect.

603. HSG told the Committee that "[the] *proscription decision of a state-linked entity such as the IRGC would be particularly complex ... I don't think that complexity has been really brought out yet in the public or indeed the Parliamentary debate that there has been*". That complexity – due to IRGC being a state organisation – is, it seems, rather more at the heart of the issue. The Home Secretary noted that any decision to proscribe would be:

> *a complex decision, that is definitely clear ... it is a state organisation, unlike many of the organisations that have been proscribed in the past, and there are lots of factors that need to be weighed up, the diplomatic implications, the implications on intelligence, the implications for the region, the military implications ...* [we would have to] *weigh up the operational benefits of proscription and the extent to which proscription would mitigate the extant threat posed by the IRGC as well as any risks posed by proscription itself.*[488]

604. Amongst our External Experts, there was a consensus against proscription, with two witnesses describing it as "*virtue signalling*". It was argued that proscription would "*have virtually zero positive effect and quite significant negative effect*". The experts cited legal considerations, and that such action would risk retaliation by Iran against UK forces in the event of a conflict. Describing "*the weaknesses of the* [UK's] *strategic handling of Iran*", External Experts viewed proscription as a continuation of the unsuccessful efforts mentioned above to "*sanction Iran into obedience ... all it does is encourage disobedience*". Without support from European allies, External Experts considered that there was no point in the UK taking this action alone as they did not consider that "*it will have any impact whatsoever*".[489]

605. We note, however, that other countries have taken such steps under their own legislation. For instance, the US government has designated the IRGC as a foreign terrorist organisation, and the Canadian government has also previously used its powers to designate the IRGC Quds Force (IRGC-QF). It is important to note that those powers are quite different from the proscription tool available to the UK Government: the UK's proscription regime is much stronger, in that it is a criminal offence to be a member of the organisation – carrying a maximum 14-year sentence. Considered in the context that around a quarter of the Iranian Cabinet are IRGC members, HSG told us that HMG would need to "*weigh up the operational benefit that a proscription decision might have in the UK ... around membership, around*

[487] Oral evidence – Foreign Secretary, 6 July 2023.

[488] Oral evidence – Home Secretary, 6 July 2023.

[489] Oral evidence – Sir Richard Dalton, 9 March 2023; Oral evidence – Professor Ali Ansari, 9 March 2023; Oral evidence – Professor Anoush Ehteshami, 9 March 2023.

glorification, for example, against the wider diplomatic factors that might come into play … we would have to consider what impact any proscription decision might have on those wider HMG objectives".[490]

606. On the question of whether proscription can be applied in respect of state actors, the Home Secretary told the Committee that:

> *on its face the terrorism definition is very broad ***. The Terrorism Act 2000 is however silent on the involvement of states in terrorism; and whether an act taken by an organ of the state is capable of being an act of terrorism.*[491]

However, the Government has previously grappled with complex proscription decisions and their diplomatic implications – for example, in respect of Lebanese Hizbollah, and the Wagner Group. This would appear to weaken the Government's argument for not proscribing the IRGC on the grounds that it is an arm of the Iranian state.

607. The Independent Reviewer of Terrorism Legislation, Jonathan Hall KC, has questioned whether or not Parliament intended for the Terrorism Act 2000 to extend to the actions of states, and in doing so has raised a legal question as to whether the terrorism definition should properly be understood to include the activities of states – which may in theory also extend to the UK's allies, even when their activities are compatible with international law. The Home Secretary told the Committee that "*successive Governments have broadly pursued a policy of non-ascription of the terrorism framework to states, instead preferring to rely on international legal frameworks for dealing with internationally wrongful acts*".[492] Nevertheless, following HMG's proscription of the Wagner Group in September 2023, senior Parliamentarians including the former Independent Reviewer of Terrorism Legislation, Lord Carlile KC, have called again for the proscription of the IRGC.

GGGG. We welcome the new National Security Act 2023, which will fill important legislative gaps in tackling state threats. However, other gaps will remain unless the Official Secrets Act 1989 is reformed. The Government now appears to be backtracking on its commitment to Parliament to take this forward: this is of significant concern given the problems with the current regime.

HHHH. No decision has yet been taken as to whether Iran would be designated under the Enhanced Tier of the Foreign Influence Registration Scheme. While there are processes to be followed, we would nevertheless be surprised if Iran were not deemed worthy of inclusion under the Enhanced Tier – if it were not, it is hard to see which countries would be.

IIII. The UK has imposed financial sanctions on 508 individuals and 1,189 entities relating to Iran. The majority of these are companies involved with the nuclear programme, but they also include sanctions for human rights issues.

[490] Oral evidence – HSG, 21 June 2023.
[491] Written evidence – Home Secretary, 26 July 2023.
[492] Written evidence – Home Secretary, 26 July 2023.

JJJJ. Given the scepticism we heard from External Experts as to the efficacy of sanctions, the Government should reconsider whether sanctions will in practice deliver behavioural change, or in fact unhelpfully push Iran towards China.

KKKK. We recognise the complexities inherent in a decision of whether or not to proscribe the Islamic Revolutionary Guard Corps. It is clear that such a decision would come with diplomatic implications: it appears that the real problem is that the Government is paralysed by the legal and practical difficulties around proscription of a state organisation – given that membership of an organisation proscribed in the UK carries a custodial sentence, which would apply to around a quarter of the Iranian Cabinet. The Government should fully examine whether it would be practicable to proscribe the Islamic Revolutionary Guard Corps and, if so, detail the competing arguments in a full statement to Parliament.

THE RESPONSE: PHYSICAL ATTACKS

608. As explored in the Threat section of this Report, since 2016 there has been a substantial increase in the threat of a physical attack by Iran on UK-based individuals, and this is now the most significant element of the Iranian threat to the UK. The Committee was told that the Home Office has policy responsibility for tackling the threat of an Iranian physical attack, and chairs a Physical Threats Outcome Group (which in turn reports to the Home Secretary) which decides the Government's approach to state-directed physical threats to UK-based individuals. The Home Secretary told us that the response to the threat of an Iranian physical attack had "*taken up increasing resource from MI5, Counter Terrorism Policing, and other law enforcement and security agencies*" and that this trend was likely to continue: "*as I see it, that is going in only one direction; I don't see that abating*".[493]

609. The Agencies' operational response to Iran's physical threat in the UK is structured (under the cross-Agency 'Iran Mission') around the following objectives:

***

Operation ***

610. An important component of the HMG response to the Iranian physical threat to UK-based individuals is a police-led process (***), which is able to *** and which seeks to reduce the risk of physical harm from *** actors to individuals based within the UK. It is currently focused on providing appropriate protection to UK-based individuals from physical threats posed to all figures at risk, according to the assessed level of risk they face.

611. This police-led process was established *** and was expanded to include protection for targets of Iranian activity ***. Since its founding, a significant proportion of the *** cases considered which have been reviewed and assessed by the process relate to Iran. Under the process, intelligence from a range of sources – which may include *** – is used to identify individuals who may be at risk of physical harm from state-backed actors, who are then subject to a risk assessment.

612. If an individual is judged to be at sufficient risk of harm, police may provide them with additional personal security advice, potentially alongside other protective mechanisms. For example, Counter Terrorism Policing (CTP) provides bespoke personal security advice to them, ***.

613. The process covers those individuals deemed to be at physical risk up to a certain level ***[494].

[493] Oral evidence – Home Secretary, 6 July 2023.
[494] ***

*Handling of higher-risk individuals ****

The police-led process (***) covers those individuals deemed to be at physical risk up to a certain level ***. If an individual is considered to be at a higher level of risk ***, then they are instead designated as ***. ***. At present, Iran *** have cases reaching this level. There are relatively few of these cases (***).

***

614. As of November 2020, there were approximately *** individuals at various stages of the process in relation to Iran – either in the process of assessment, or receiving support from the programme. These individuals are primarily UK-based Iranian individuals who are part of a variety of dissident groups, and many of these individuals ***.

615. The Committee was provided with updated figures during the course of the Inquiry. As at 1 June 2023, there had been *** cases considered in relation to Iran – a very significant increase since November 2020. Of those, *** were assessed to be of a lower threat, *** assessed to be of a greater threat and *** were still undergoing assessment. It appears therefore that the level of physical threat is broadly comparable with that which we saw during our Russia Inquiry.

616. HSG originally told the Committee that *** individuals were judged to be at a higher level of risk, and therefore managed outside of this process (as set out in the box above). The Home Secretary, however, told the Committee:

> *we have a high number of people in comparative terms: we have *** individuals, who are under the highest level of protection ... costing us* [a considerable amount] *** *in the protective security arrangements that are required to keep those individuals safe.*[495]

It was unclear from the Home Office which figure is correct.[496]

617. HMG described the police-led process as a useful way to categorise individuals at risk, take decisions about the comparative level of threat and identify those who require *** intervention. In terms of the overall success of the programme, HMG told us that: "*we have been pretty successful by the people we have been advising*" – although it was noted that individuals in other countries have not always chosen to follow advice they have been given:

> ***[497]

[495] Oral evidence – Home Secretary, 6 July 2023.

[496] As at January 2024, the Home Office told the Committee that the correct number was ***, and that the reason for the discrepancy was an error in their evidence to the Committee, which they then failed to pick up when asked to check the accuracy of their evidence. Given the importance of this issue, we found this failure to provide reliable evidence to the Committee disappointing.

[497] Oral evidence – ***, *** June 2023.

618. The Committee was told that the Home Office had conducted a review of HMG's understanding of state-directed physical threats to UK-based individuals and the structures in place to respond. The review had concluded that the level of threat from countries other than *** Iran was at the lower end of the physical threat spectrum and did not currently justify increasing resource on the police-led process (***). In November 2021, the Home Secretary agreed with the review's recommendations that the process should remain focused on *** Iran given the disproportionate threat they pose, and on the most severe physical threats of assassination and kidnap.

Assassination

619. As explored in depth in the Threat section, MI5 has seen "*increasing intent by the Iranian Intelligence Services to conduct a lethal operation in the UK*", and at least 15 attempts at murder or kidnap against British nationals or UK-based individuals since the beginning of 2022.[498] In some cases, MI5 and CTP have identified threats to particular individuals and provided advice not to travel, which has addressed the threat. In other cases, swift action has been required to respond to "*sharper*" threats: for instance, in early 2023:

> *police colleagues arrested a man who had conducted some hostile reconnaissance of the Iran International headquarters building in west London. When he was arrested, he had in his possession some video footage that he had taken that day. He flew into the UK that morning but he had also on the same phone ... video footage that had clearly been provided to him by somebody else who had undertaken some hostile reconnaissance of the same facility on an earlier occasion ... the man I think has now been charged under Terrorism Act offences.*[499]

Operation ANISE

Operation ANISE was an investigation into the Iranian Intelligence Services (IIS)-directed assassination plots against Iranian dissidents in Europe, carried out by a criminal network run by narcotics trafficker and IIS agent Naji Sharifizindashti, an Iranian national based in Turkey.

Between 2018 and 2019, UK and European law enforcement and intelligence agencies carried out a number of disruptions of Sharifizindashti's criminal network. HMG subsequently instigated a number of actions which had a significant disruptive effect.

In January 2019, the UK and European partners issued a démarche to the Iranian Ministry of Foreign Affairs, holding the Ministry of Intelligence and Security (MOIS) responsible for the murders of three Iranian dissidents in Europe between 2015 and 2017. HMG provided Iran with evidence of Iranian culpability, ***. The démarche also outlined other individuals deemed to have direct involvement in the assassinations.

[498] MI5 Quarterly Report, July–September 2022; Oral evidence – MI5, *** June 2023.

[499] Oral evidence – MI5, *** June 2023.

***

. HMG told us that the démarche had been "" and that as a result ***[500] *** It appears therefore that the impact of the ANISE disruptions of Iranian hostile activities against Iranian dissidents was ***.

Kidnap and lure operations

620. HMG told the Committee that one of the outcomes of Operation ANISE may have been the increase in attempts ***

> *One possible shift that may in part have been influenced by that démarche is that, comparatively speaking in the years since, we have ***.*[501]

621. ***. We asked what ***: ***.[502]

622. The Committee was told about a case in *** when a member of the Iranian diaspora received reports of being targeted by the IIS. An MI5 investigation assessed that a lure attempt was probably being made – an Iranian individual *** had made contact with the target ***. We were not provided with further detail as to whether MI5 had intervened in this case; however, the UK resident in question has ceased all contact with the individual.

Operation MACE

During ***, MI5, working closely with CTP, the Home Office and GCHQ, investigated the targeting of a UK-based dual UK–Iranian national ***.

Intelligence indicated that the targeting was intended to support future operational activity – possibly a physical threat. The targeting included ***.

The Committee was not told whether MI5 had intervened in this case, or whether the investigation was ultimately successful in preventing this targeting.

623. In addition to action taken in relation to specific threats to individuals – such as those detailed above – MI5 also takes disruptive action (with domestic and international partners) in relation to a broader threat. One such example – which resulted in arrests under the Official Secrets Act 1911 – is detailed below.

[500] Oral evidence – ***, *** June 2023.
[501] Oral evidence – ***, *** June 2023.
[502] Oral evidence – MI5, *** June 2023.

Operation NUTMEG

As referenced in the Threat section of this Report, in 2020, MI5 investigated a UK-based Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) agent network which was reportedly gathering intelligence against Israeli or Jewish targets.

In terms of the response, MI5 sought to disrupt the UK-based network and later in 2020 the *** principal Subjects of Interest (SOIs) were arrested under the Official Secrets Act 1911. ***

MI5 assesses that the disruptions had the desired effect on the network, and MI5 has ***. The SOIs ***.

LLLL. The primary mechanism by which the Government responds to the Iranian physical threat is * a police-led process. We note the significant increase in the number of cases considered relating to Iran, and the successes of the operation in providing advice and protection.**

MMMM. The Committee was provided with numerous examples illustrating the increasing intent by the Iranian Intelligence Services to conduct lethal operations in the UK: we commend the efforts of MI5 and the police in response to what is now a serious threat.

NNNN. Given that Iran does not view attacks on dissident, Jewish and Israeli targets in the UK as constituting attacks on the UK, we encourage the Government and its international partners to make it clear to Iran – at every opportunity – that such attacks would indeed constitute an attack on the UK and would receive the appropriate response.

THE RESPONSE: ESPIONAGE

624. As noted in the Threat section of this Report, since 2020, the Intelligence Community have assessed Iranian espionage – whether human or cyber – to pose a significant threat to the UK and its interests (although from the evidence that the Committee received, it appeared that the Iranian espionage threat is smaller in scale than that posed by Russia and China, as explored in the Committee's previous *Russia* and *China* Reports).

625. Under the cross-Agency 'Iran Mission', the Agencies' response to Iran's espionage activity in the UK is structured around the following areas:

***

626. This response appears to focus on tackling ***: there are ***. *** objectives referring to 'cyber' relate to ***. However, we have considered the Agencies' work to tackle cyber espionage under the same broad headings: understanding; investigating and disrupting; and hardening.

Tackling human espionage

(i) Understanding

627. As explained previously, the Iranian espionage threat may not necessarily follow a set strategic plan and may be more opportunistic, which to some extent explains the ***. The Home Secretary told the Committee that the Intelligence Community were working to "*increase our understanding of* ***"[503]; however, we were not provided with any further detail beyond this – and it appears to be aspirational rather than a main priority, in terms of espionage.

Academia

An area where Iran's strategic intent is clear is its attempts to acquire material and knowledge from UK industry and academia to support the development of its military and other dual-use capabilities, including those relevant to the nuclear programme. The Committee was provided with specific examples of targeted action to counter these attempts:

- In ***, an Iranian scientist sought to collaborate with a UK university to build ***. On the basis that this would probably have supported Iran's weapons programme, *** the Intelligence Community advised the university against the project.
- The National Protective Security Authority runs the 'Trusted Research' initiative, with support from the National Cyber Security Centre (NCSC). This aims to raise awareness amongst universities of threats from Iran – amongst other state threats – and works with academic institutions to incorporate additional capabilities to defend the sector.

[503] Oral evidence – Home Secretary, 6 July 2023.

- ***, SIS and GCHQ provided intelligence to inform a decision to *** complete academic studies. This supported counter-proliferation efforts by the Ministry of Defence (MoD), to prevent the spread of technical expertise to countries of concern.
- HMG investigates specific cases of students seeking to study in the UK who are considered a potential risk. HMG also uses export controls to seek to manage the export of sensitive areas of research which could be exploited by Iran.
- The Foreign, Commonwealth and Development Office (FCDO) and the Department for Science, Innovation and Technology established the Research Collaboration Advice Team and broadened the Academic Technology Approval Scheme in 2021, to prevent knowledge transfer relating to Critical National Infrastructure (CNI). Proposals for students and academic bodies are screened in order to counter efforts by threat actors to acquire sensitive knowledge. In 2023, the Integrated Review Refresh announced a Review of Academic Security to assess whether further national security measures are required in this area.

(ii) Investigating and disrupting

628. Regardless of whether there is any underlying strategic intent, Director General MI5 was clear that, "*given the frequency with which the Iranians are trying to do things here, they clearly regard the UK as an environment in which they are still determined to have effect*".[504]

629. As with all of its work to counter state threats, MI5's objectives are to "*seek those trying to pass sensitive UK information and equipment to other countries and ensure they don't succeed*" (counter-espionage) and to "*disrupt the actions of foreign intelligence officers where these are damaging to our country's interests*" (counter-intelligence).[505] MI5's counter-espionage work is reliant on information collected either from its own activities or provided to it by external sources. The Director General described its system for processing new information:

> *that would go through the usual triage process: how much do we believe this? How immediate is the risk? How credible is the sourcing? All those classic professional intelligence judgements. Typically ... it would be taken on by a sort of combined team ... where bits of MI5, bits of GCHQ and others, police, depending on the nature of the activity* [teams] *would come together and make a judgement.*[506]

Director General MI5 explained that the earliest stages of an investigation are often the most difficult:

> *So the teamwork within the UK works well on those occasions when we find some initial lead to what is going on. That is often the hardest part, trying to spot*

[504] Oral evidence – MI5, *** June 2023.
[505] MI5 website.
[506] Oral evidence – MI5, *** June 2023.

> *in the first place these bits of activity, because, you know, clearly UK business people, academics, are highly available, especially online these days, and so the Iranians, just like the Russian and Chinese, have many, many opportunities to dangle potentially tempting conference invitations, phishing emails, whatever it might be.*[507]

630. In September 2021, we were told that MI5 had *** staff working on state threats, and *** working on Iran specifically. While part of their work focuses on investigating and disrupting UK-based Iranian Intelligence Services (IIS) agent networks, the Director General highlighted that this work is much broader than countering traditional espionage operations: he told the Committee that MI5 will often use its "*traditional counter-terrorism toolkit*" more than it would against conventional state threats, ***. He noted that "*clearly Iran to some extent straddles the boundary between conventional state threats and counter-terrorist work*".[508]

631. *** a unit in the Home Office called the Special Cases Unit (SCU). The Home Office explained how this unit works to co-ordinate efforts across Government:

> *the way we integrated our immigration tools and indeed our wider toolkit against state threats and counter-terrorism is crucial with *** the Home Office's Special Cases Unit. We have a dedicated unit that looks at using those immigration tools to ensure people either cannot access the UK in the first place, or if they are here, that they are removed ... It obviously applies across the full range of state threats but, as I said, we are increasingly putting that towards the Iranian threat.*[509]

*** the SCU is able to use a range of immigration tools to disrupt agent networks. (We have explored earlier in this Report the deficiencies in the Official Secrets Act 1989, which make successful prosecutions of hostile actors in the UK – such as Iranian agents – under espionage laws more difficult.)

632. In the first instance, the SCU has several means of denying individuals entry into the UK. For example:

- Exclusions and deprivations: The power to exclude foreign nationals from the UK or revoke British citizenship (the latter can also be applied in cases where the individual is in the UK) when such action is assessed to be conducive to the public good or the individual is considered to pose a threat to the public. HSG told us that:

  > *We had the *** use of the Royal Prerogative to remove a British passport from an individual *** ... We have deprived *** individuals of their British nationality who were judged *** deprived in *** and the other in ***.*[510]

[507] Oral evidence – MI5, *** June 2023.
[508] Oral evidence – MI5, *** June 2023.
[509] Oral evidence – HSG, 21 June 2023.
[510] Oral evidence – HSG, 21 June 2023.

HMG also told us that between December 2018 and June 2023, the SCU had excluded *** on national security grounds.

- Visa refusals/revocations: The power to refuse an entry clearance application or to revoke entry clearance or permission held, under the Immigration Rules.
- Temporary exclusion orders: The managed return of British citizens who are suspected of involvement in terrorist activity abroad. HSG told the Committee that it had "*used recently the Temporary Exclusion Order power against an individual who *** ... for counter-terrorism reasons ...* [and] *that is a good example of them straddling both terrorism and state threats*".[511]

633. The SCU also has a number of powers which it can use to disrupt agent networks by taking action against individuals who are already in the UK. For example:

- Refusal of British citizenship: Where there is adverse information concerning an individual's background that suggests that they may not be of good character.
- Exclusions from the Refugee Convention: Excluding individuals from eligibility for refugee status.[512]
- Immigration detention: Detaining an individual on national security grounds where HMG is actively working to enforce removal in a reasonable timeframe.
- Enforced deportation: Deportation owing to an individual being excluded from eligibility for refugee status under the Refugee Convention, where there are no barriers to their removal under Articles 2 and 3 of the European Convention on Human Rights (ECHR); or a foreign national offender who has been served with a deportation order.
- Deportation with assurances: Bespoke agreement with the country of origin to deport an individual with the assurance that removal will not result in a breach of Articles 2 and 3 of the ECHR.
- Restricted leave: A form of limited leave outside the Immigration Rules, granted to individuals who are refused refugee leave or humanitarian protection on the grounds of serious criminality or their conduct, character or associations, but who cannot be removed because it would breach their human rights.
- Electronic monitoring or tagging: A stringent form of immigration bail, which enforces a curfew.

[511] Oral evidence – HSG, 21 June 2023.

[512] Under Article 1F of the Refugee Convention, individuals may be excluded from eligibility for refugee status if they have committed any of the following: war crimes or crimes against humanity; a serious non-political crime prior to admission to the UK; acts contrary to the purpose and principles of the UN.

Disruptive immigration tools in action

In *** was assessed to be an IIS agent. They were believed to have passed information to the IIS on ***. The SCU excluded them from the UK on the grounds that their presence in the UK was not conducive to the public good on national security grounds. They had an existing *** visa which was revoked on the back of the exclusion.

*** was assessed to be an IIS recruitment target and ***. Between *** they had been issued visas to visit the UK before the increase in threat from Iran. Their application for a *** visa was refused under the Immigration Rules, on the grounds of national security in that their presence in the UK would not be conducive to the public good.

(iii) Hardening

634. Immigration tools are a useful means to help ensure the UK is a "*hard operating environment*" for foreign agents and operatives – i.e. that Iran, and other countries, are deterred from conducting espionage in the UK because it is too difficult to do so. Another tool the Intelligence Community use is to provide briefings and protective security advice to certain individuals based in the UK but who travel to more permissive third-country environments, where *** they might be targeted by Iran. Director General MI5 told the Committee that:

> *we try to approach that end of the market through briefings, protective security advice, raising awareness, the kinds of things that you would expect.*[513]

635. Director General MI5 told the Committee that it considered the Government's use of disruptive immigration tools and protective briefings to be successful in demonstrating to Iran that the UK is a hard operating environment:

> *I think it is probably fair to say that the Iranians do regard the UK as a comparatively difficult operating environment ...* [and] *** *in a number of cases.*

Nevertheless, regarding Iran's overall attempts to operate in the UK, the Director General told the Committee that:

> *I don't think they think we are the easiest place for them to operate, but they are still seeking to operate here.*[514]

[513] Oral evidence – MI5, *** June 2023.

[514] Oral evidence – MI5, *** June 2023.

Tackling cyber espionage

636. Iran also poses a significant cyber espionage threat and, as noted above, it may be useful to consider similar strands of work to tackle it as for the human espionage threat.

(i) Understanding

637. The dynamic nature of Iran's cyber activity clearly could pose a challenge in terms of developing a clear understanding of its strategic intent. When we asked GCHQ, it told the Committee that:

> *there are a number of different organisations within Iran, some of which are completely owned and run by the state, and some of which are affiliated, and there is a crossover with criminal cyber activity ... *** ... in this instance for espionage purposes as well.*[515]

638. The Joint State Threats Assessment Team (JSTAT) provided the Committee with specific examples of ***.

(ii) Investigating and disrupting

639. As described in the Committee's 2015 Report on Privacy and Security, the Agencies use a range of methods and sources to obtain information and to conduct investigations across the different areas of their work (including, for example, Iranian cyber espionage activity). These include:

- Interception of internet and telephony communications: This data comes from a combination of targeted interception overseas (e.g., such as from ***) and working with telecommunications operators in the UK who, under the authority of interception warrants, provide the Agencies with access to communications as they traverse their networks.
- Interception of communications from other traditional channels: This may include communications satellites, microwave transmitters and radio signals.
- Intelligence collection via equipment interference: This relates to the gathering of communications or other information by interfering with equipment such as computers, phones and other electronic devices. It can range from remotely accessing computers and other electronic equipment to covertly downloading the contents of a mobile phone or storage media.
- Data acquisition and analysis: Using open source and covertly acquired datasets (such as bulk personal datasets) and data obtained by Intelligence Community partners.
- Interception by the National Technical Assistance Centre: This involves GCHQ's wider support to law enforcement and the wider Intelligence Community and includes: interception of communications on behalf of domestic bodies, particularly law enforcement; forensic examination of seized computer equipment; and

[515] Oral evidence – GCHQ, *** June 2023.

requesting access to communications from telecommunications operators in the UK (subject to the appropriate warrants).

640. MI5 provided the Committee with a few specific examples of its work to help tackle Iranian cyber espionage – for example, gathering intelligence ***. This understanding informs GCHQ operations to counter Iranian activity, which may include operations ***. For example, the Committee was told that in ***.

Operation PAPRIKA

In ***, NCSC investigated the penetration of *** internal systems by an Iranian state-sponsored threat group, PEPPER. PEPPER was judged to have gained access to the *** internal networks,[516] effectively providing it with access to bulk personal data. This data could have been used by the IIS to understand *** patterns and therefore support their counter-intelligence operations.

NCSC worked closely with the *** to draw up a plan to fix this vulnerability. This plan was implemented in *** and included the ***.

The Intelligence Community judged the implementation of this plan to have been a success, denying the means by which PEPPER was able to access the *** networks.

(iii) Hardening

641. As explored in the Threat section of this Report, the Iranian espionage threat manifests itself acutely in the cyber domain, since cyber espionage enables the IIS to gain information which would often not be possible to obtain within countries – such as the UK – due to the difficult operating environment. Making the UK's cyberspace an equally difficult operating environment must therefore be a key strand of the Government's work to counter the Iranian espionage threat.

642. In the 'Offensive Cyber' chapter, we explore some of the ways in which HMG (through GCHQ, NCSC and the National Cyber Force) is working to harden the UK's cyber defences, including bolstering UK resilience to Iran's cyber activity through engagement with cyber security partners and outreach to industry sectors, and running the Active Cyber Defence programme to provide technical protection to important national networks. This work to strengthen the overall level of cyber security and resilience across the whole of UK society is central to the 2022 National Cyber Strategy, which emphasises a whole-of-society approach to cyber resilience in the UK. GCHQ told the Committee that it considered that the National Cyber Strategy had had a positive impact, and that the whole-of-society approach "*has been a real boost to the efforts the NCSC have been making for a number of years*".[517]

[516] By comparing the evidence received by the Committee relating to this Inquiry and GCHQ's Quarterly Report, *** it was clear that *** specifically was one of the *** compromised.

[517] Oral evidence – GCHQ, *** June 2023.

643. Using this whole-of-society approach, NCSC works with industry and key sectors to build their resilience to cyber operations. This work includes a Cyber Assessment Framework against which companies can check their levels of cyber security, and public advice – for instance, at the most basic level, advising individuals to use a range of different passwords. Despite this work, even when an espionage target is relatively obvious – such as the UK Parliament – NCSC is not always able to prevent Iranian cyber espionage operations. When the Committee questioned why the Intelligence Community had been unable to anticipate and stop the cyber-attack on Parliament in 2017 (for which the BBC reported that UK civil servants had accused Iran of being responsible), GCHQ said:

> *** *... We have also done a huge amount of work* [since] *on raising the level of cyber resilience, including directly with MI5 and other colleagues, with Parliament itself, to ensure that Parliamentary digital services are much better protected from this sort of cyber threat in future.*[518]

644. The Committee was told about some of the more active tools and capabilities that NCSC and GCHQ use to build the UK's resilience to the Iranian cyber threat, for example:

> *a protective DNS* [Domain Name System] *service*[519] *... with a commercial partner ... that works to government but we also extended it to the wider public sector, including the health sector, during the pandemic. All of the threat information we have on Iranian cyber threats will go into that service to make sure that, if somebody tries to click on a link that we have identified as an Iranian cyber threat, it will get blocked by this service that we run so they can't access it.*[520]

OOOO. The use of tools such as protective briefings and disruptive immigration measures has been successful in demonstrating to Iran that the UK is a hard operating environment. However, that has not stopped it from seeking to operate agent networks here.

PPPP. The Iranian espionage threat manifests itself acutely in the cyber domain, since cyber espionage represents an easier way for Iran to gain information which it would not necessarily be able to obtain within the UK due to the difficult operating environment.

[518] Oral evidence – GCHQ, *** June 2023.

[519] A DNS service translates text-based website addresses (such as www.gov.uk) into numerical Internet Protocol (IP) addresses (such as 192.0.2.1). The DNS service therefore acts similarly to a 'phonebook' by identifying which website names link to which IP addresses.

[520] Oral evidence – GCHQ, *** June 2023.

THE RESPONSE: OFFENSIVE CYBER

645. Under the 2022 National Cyber Strategy, the Home Office is the policy lead for the Government's work to detect, disrupt and deter state threat actors from offensive cyber activity against the UK. The Home Office told the Committee that it works with the Ministry of Defence (MoD), the Foreign, Commonwealth and Development Office (FCDO), and a wider community including the Agencies and law enforcement, and that it co-ordinates delivery through a 'Threat Pillar Board' which aims to bring coherence to the UK's response. While the policy and a co-ordinating role lies with the Home Office, the operational response lies with GCHQ, the National Cyber Security Centre (NCSC) and the National Cyber Force (NCF). The four key areas of work for them are:

(i) to understand Iranian Intelligence Services (IIS) cyber capabilities and intent towards the UK and its allies;

(ii) to bolster UK resilience to IIS cyber activity through engagement with cyber security partners, outreach to industry sectors and the incident management process;

(iii) to run the Active Cyber Defence programme to provide technical protection to important national networks; and

(iv) to raise the cost to IIS of their cyber activity via overt and covert means.

(i) Understanding Iranian offensive cyber activity

646. As outlined earlier in the 'Defending the UK' chapter, NCSC is the UK's technical authority on cyber security, and works to prevent, disrupt and investigate cyber threats – including those posed by Iran.

647. NCSC gathers intelligence on the Iranian threat, to develop knowledge of the Iranian intent, capabilities and individuals involved, and to identify the actions carried out by Iranian-linked *** cyber units. This intelligence is then used to inform NCSC and NCF's strategic plans to counter the threat.

(ii) Bolstering resilience

648. GCHQ told the Committee that a key strand of activity is "*just raising the resilience bar more generally so that it is less likely that* [Iran's] *** *attacks will be successful*".[521] ('Raising the resilience bar' in this context means strengthening the overall level of cyber security and resilience across the whole of UK society.) To do this, NCSC combines intelligence and insight from across the Intelligence Community to provide advice and guidance to academia, Critical National Infrastructure, industry, Government and the UK public. This aims to increase awareness of the cyber threat and help organisations to strengthen their defences and become a harder target for hostile cyber activity. A key element of this work is NCSC's Cyber Information Sharing Platform, which is accessible to a wide

[521] Oral evidence – GCHQ, *** June 2023.

range of organisations across society and through which NCSC issues information on the cyber threat in real time. When incidents do occur, NCSC responds to minimise harm to the UK, assisting organisations with recovery and ensuring that lessons are learnt for the future.

649. The Committee was told that, through this work, NCSC has illuminated tools and techniques used by Iranian cyber groups, clarified these cyber groups' objectives and warned UK organisations that are targeted. Specific examples which the Committee was provided with include:

- advisories issued by NCSC that have warned of the threat from spear-phishing, Islamic Revolutionary Guard Corps (IRGC) ransomware activity, and cyber activity associated with the Ministry of Intelligence and Security (MOIS);[522]
- in 2021, NCSC identified that an online domain had been set up by the IRGC to spoof the website of a think tank, and prevented this from being used for malicious purposes;
- in 2021, NCSC discovered that ***; and
- in ***, NCSC took action against the Iranian cyber group known as ***. As a result, NCSC was able to understand and disrupt the threat ***.

650. The Committee was also provided with the following examples of GCHQ work to build resilience against Iranian offensive cyber activity:

- having identified Iranian malign cyber activity in the Middle East, GCHQ notified the organisations which had been compromised, and published information on the Iranian threat so that organisations had the knowledge to take cyber defensive action; and
- exposure of *** malware capability and the fact that it had been used against ***. This work aimed to increase awareness of Iran's irresponsible use of cyber capabilities and to undermine Iranian cyber groups.

Resilience of Critical National Infrastructure

651. With regard to the resilience of Critical National Infrastructure (CNI) specifically, GCHQ told the Committee that it has a team that works with the National Protective Security Authority (NPSA) "*to raise the standard of cyber resilience and security in the CNI ... not just in response to the Iranian threat but also the Russian, Chinese and the ransomware criminal threat that we have identified*".[523]

652. NCSC also provides a Cyber Assessment Framework which organisations can use to assess their level of cyber resilience. The Committee was told that many policy departments

[522] Written evidence – HMG, 12 July 2023.

[523] Oral evidence – GCHQ, *** June 2023.

and regulators insist that CNI operators use this framework, which means that GCHQ has "*really good data about the level of their cyber resilience but can then track how they are improving that over time*".[524] However, this is not mandatory for all CNI operators.

653. The Deputy National Security Adviser (DNSA) described the National Cyber Strategy as having a "*galvanising effect*" with regard to cyber security of CNI, but stated that:

> *it is not something we are sleeping on … the risk to our cyber security and our cyber resilience of Critical National Infrastructure is something that we continually have to monitor and we are considering setting some really quite ambitious targets for all CNI to implement by 2025.*[525]

Nevertheless, the Foreign Secretary was candid: "*Does more need to be done? I suppose the simple answer is yes*".[526]

(iii) Active Cyber Defence

654. NCSC operates the UK's Active Cyber Defence programme, which aims to reduce the harm from cyber-attacks by providing organisations with tools and services that provide protection from a range of attacks. The Active Cyber Defence programme focuses on tackling the more common attacks that affect people's everyday lives, rather than highly sophisticated and targeted attacks, which NCSC deals with in other ways (for instance, by building organisations' overall resilience, as covered above).[527]

655. Some of the services which NCSC offers to organisations through its Active Cyber Defence programme include:

- Early Warning: This helps organisations investigate cyber-attacks on their network by notifying them of malicious activity that has been detected in information feeds.
- Exercise in a Box: This is a toolkit containing realistic scenarios that helps organisations practise and refine their response to cyber security incidents in a safe and private environment.
- Mail Check: This enables organisations to assess their email security compliance and adopt secure email standards which prevent criminals from spoofing their email domains.
- Web Check: This helps organisations find and fix common security vulnerabilities in the websites that they manage.
- Check your Cyber Security: With this, organisations can run instant checks on their cyber security, including whether their web browser is out of date, whether the privacy of their emails is protected and whether cyber criminals could attack systems via the internet to gain data.

[524] Oral evidence – GCHQ, *** June 2023.
[525] Oral evidence – NSS, *** June 2023.
[526] Oral evidence – Foreign Secretary, 6 July 2023.
[527] 'Active Cyber Defence', NCSC website, accessed 20 October 2023.

(iv) Raising the cost

Public attribution of cyber-attacks

656. An important strand of work in defending against Iranian cyber-attacks on the UK is to deter Iran from conducting such attacks in the first place – the Agencies therefore seek to raise the cost to Iran of it launching a cyber-attack on the UK. One way to deter Iranian activity is the public attribution of attacks to Iran – for example, following the 2022 Iranian cyber-attack on the Albanian government.

Public attribution of cyber-attack on the Albanian government

As noted in the Threat section of this Report, in July 2022, Albanian online government services were hit by a large-scale cyber-attack designed to destroy data and disrupt systems. The attack disrupted essential government services, including payment of utilities, medical appointment booking and schoolchildren enrolment.

Microsoft technical analysis confirmed links between the networks affected and Iranian-associated cyber infrastructure. The Albanian government publicly blamed Iran for this series of attacks and consequently severed diplomatic ties with Iran.

NCSC judged with high confidence that Iranian state-linked cyber actors were almost certainly responsible and, as such, the UK joined Albania and the US in publicly attributing the attack to Iran.[528] This was the first time that the UK had publicly attributed a destructive cyber-attack to Iran.[529]

657. GCHQ considers public attribution of cyber activity to be a "*really useful tool*",

> *to ensure that as many people as possible can then mitigate the risk. That will often take an entire category of capability away from the Iranians ...* ***.[530]

As GCHQ notes, public attribution generally is not without risk, since it may help adversaries to identify how the Intelligence Community have detected and countered a cyber-attack – and then to improve their capabilities to avoid this in future. GCHQ told us that this was "*a really acute issue*": in retrospect, some of its earlier interventions to disrupt cyber threats *** could theoretically have demonstrated GCHQ's understanding of the deficiencies in how attackers operate, thus making it easier for adversaries to fix such deficiencies. This trade-off was also demonstrated in Operation SAFFRON.

[528] 'UK Condemns Iran for Reckless Cyber Attack against Albania', Press release by the FCDO, 7 September 2022.

[529] GCHQ Quarterly Report, July–September 2022.

[530] Oral evidence – GCHQ, *** June 2023.

Operation SAFFRON: Mabna Institute

A joint UK–US operation (*** the FBI) was conducted to counter the offensive cyber threat from the Iranian state-linked cyber group known as the Mabna Institute (judged to be responsible for a global cyber espionage campaign targeting universities ***). The disruption was led by an FBI indictment of the actors but also involved FCDO public attribution *** (although the Committee was not provided with detail on what this meant in practice or the impact it had).

The operation was effective in immediately halting the actors' activity, but not without cost ***. It led to an improvement in ***.

658. Taking into account the trade-offs of disruption operations such as SAFFRON, GCHQ routinely assesses whether its operations will help its adversaries to improve their capabilities or lead to longer-term degradation. GCHQ explained:

> ***.[531]

Cyber deterrence

659. While the UK has been publicly 'calling out' cyber-attacks for a number of years, the FCDO has more recently conducted a review of cyber deterrence more broadly to see how it can support UK policy on imposing costs on states for malicious cyber activity. Ministers were presented with five recommendations to endorse – namely to:

(i) strengthen the governance of cyber campaigns to better integrate thematic and geographic policy goals;

(ii) create a baseline of measuring the effectiveness of different tools;

(iii) update HMG guidance on responding to state-directed malicious cyber activity;

(iv) deepen and broaden HMG's network of international partnerships for deterring malign activity, to amplify impact and reduce risk of escalation or retaliation; and

(v) continue HMG efforts on cyber governance to establish the rules and norms of acceptable state behaviour in cyberspace.

Ministers were also presented with the following four further issues to consider:

(i) the use of criminal charges against overseas cyber actors including ***;

(ii) HMG's approach to cryptocurrency, ***. HMG could explore options to amplify its ability ***;

(iii) the risk appetite for ***; and

(iv) whether NCF should ***.

[531] Oral evidence – GCHQ, *** June 2023.

However, at the time of writing (October 2023), the Committee had not been told whether Ministers were still considering these recommendations and additional issues, or what action had been agreed to address them.

660. The Committee asked the Intelligence Community to what extent the UK's own offensive cyber capability acted as a deterrent towards Iran. GCHQ told the Committee that:

> *it is really important we don't consider cyber deterrence as a specific thing, that you use offensive cyber to deter cyber-attacks coming to you ... Cyber deterrence does not work in the same way as a nuclear deterrent.*[532]

The Foreign Secretary agreed, emphasising that:

> *our position is to prioritise non-aggression. It is there for a reason, it is there if we need it, but it is not our go-to option and we recognise that ... it must naturally form part of a broader arsenal of activity.*[533]

National Cyber Force activity

661. The NCF was established in 2020 and has specific responsibility for UK offensive cyber activity. GCHQ described the NCF as a "*big asset*" and "*a clearly structured way of conducting offensive operations in response to things like Iranian threats*".[534] In relation to Iran, the Committee was told that the NCF ***.

662. The Intelligence Community provided the Committee with specific examples of NCF operations ***:

- Operation SESAME – a bilateral operation with *** with the aim of ***; and
- Operation TAMARIND – the NCF actively degraded ***.

663. Despite these examples, the Committee was told that due to the low cost and ubiquity of cyber-attacks, GCHQ and NCSC are required to invest significant time and resource in understanding the target, before considering how to respond effectively. The Committee recognises the importance of this – and the Foreign Secretary's insistence that "*the diplomatic bit ... deterring, dissuading, increasing the perceived cost of actions like this, is our best form of defence, rather than retaliatory*".[535] However, we are concerned as to whether the UK is sufficiently leveraging its own offensive cyber capability against Iran: the Committee was told that in the 12 months ***, the Intelligence Community had successfully concluded ***. The Committee was also told that in the same time period the Intelligence Community *** counter-cyber operations against Iran (i.e. operations to disrupt Iranian cyber-attacks) – which appears to be a further illustration of the low priority accorded to cyber work on Iran.

[532] Oral evidence – GCHQ, *** June 2023.
[533] Oral evidence – Foreign Secretary, 6 July 2023.
[534] Oral evidence – GCHQ, *** June 2023.
[535] Oral evidence – Foreign Secretary, 6 July 2023.

QQQQ. It is essential to 'raise the resilience bar': if there is good cyber security and resilience across the UK, then it is less likely that Iran's * cyber-attacks will be successful. The National Cyber Security Centre's work to illuminate the tools and techniques used by Iranian cyber groups, and to warn UK organisations that they are being targeted, is therefore key to defending the UK.**

RRRR. The Committee has previously expressed concerns about Government complacency in allowing Russian pre-positioning for an attack through widespread penetration of UK Critical National Infrastructure. It is vital that the same mistakes are not made in relation to Iran – particularly given Iran's proven capability to cause serious disruption to essential services.

SSSS. The UK must raise the cost to Iran of it launching a cyber-attack on the UK, so as to deter it from doing so: public attribution of attacks is a valuable tool (albeit not without risk).

TTTT. The National Cyber Force was established in 2020 with specific responsibility for offensive cyber activity. Such operations have *. The Committee recognises the time and resource required in mounting such operations.**

UUUU. The Committee was surprised to hear that the Intelligence Community had successfully concluded * counter-cyber operations against Iran (i.e. operations to disrupt Iranian cyber-attacks) in the 12 months ***.**

664. The Committee was told that the policy response to countering Iranian interference is led by the Cabinet Office and co-ordinated through a Cabinet Office-led Board – the Foreign Interference Outcome Group (FIOG). The FIOG is responsible for taking forward the actions and recommendations of the 'Review of Interference' – a cross-Government review led by the then Deputy Director General MI5, working to the National Security Adviser – which was designed "*to further build our understanding and resilience against the interference threat*".

665. However, there are a number of departments which appear to be leading work under the interference 'banner'. For example, a separate cross-Government working group will "*scope the impact of malign Iranian influence and interference in the UK, potential levers to counter this activity, and contingency planning for escalatory events*".[536] This work will cover issues such as cultural centres, educational facilities, academic collaboration and Iranian information operations. The Department for Science, Innovation and Technology also has responsibility for counter-disinformation policy, and in addition, in November 2022, the Government announced the establishment of the Defending Democracy Taskforce – a cross-departmental and inter-Agency initiative chaired by the Security Minister within the Home Office. It is unclear how the work of these bodies and reviews differs and to what extent there is duplication.

The Defending Democracy Taskforce

666. The Home Secretary told the Committee that the Defending Democracy Taskforce:

> *is focused on establishing a clearer picture of the nature of the threat, I think this is an emerging issue that we are grappling with in recent months and so we are trying to establish and clarify exactly what the nature of the threat is but then also, importantly, build resilience and co-ordinate. So that is what it is doing, in one word, it is co-ordinating.*[537]

In that respect, the Committee notes, again, the tendency to establish too many bodies to co-ordinate, at the expense of those bodies doing the actual front-line work. Despite asking on a number of occasions, the Committee was not provided with any concrete outcomes that the Defending Democracy Taskforce has been responsible for achieving since it was established. It is unclear whether it represents a step forward in the Government's approach or simply yet another co-ordinating structure.

667. When we asked the Home Secretary for more detail on the Taskforce's work relating to Iran specifically, she told the Committee that it operates on an actor-agnostic basis, but that all of its workstrands were relevant to Iran. She described three key workstrands:

> *One ... is the increased cyber offer to Parliamentarians which we are working with Parliamentary security on.*

[536] Written evidence – HMG, 25 August 2023.

[537] Oral evidence – Home Secretary, 6 July 2023.

> *The second is the work around the security of elections ...*
>
> *The third is to build our understanding of transnational repression ... in terms of the Iranian diaspora ... an area where we have less visibility and that is something we want to build and we want to understand how that is impacting on communities.*[538]

(i) Protecting Parliamentarians and decision-makers

668. As noted earlier in this Report, the Committee was told that the majority of Iranian interference that HMG had seen were attempts to shut down dissidents or Farsi-language media organisations. On the question of political interference, HMG told the Committee that whilst Iran "*maintains the intent to conduct political influence and interference activity, it is not an area where we believe that Iran has had significant impact to date*".[539] However, it noted that this may change in future, as the Iranian Intelligence Services (IIS) improve or they learn from others.

669. In terms of the practical steps currently being taken to protect Parliamentarians and decision-makers, the Committee was told that the National Protective Security Authority, the National Cyber Security Centre (NCSC) and MI5 work with the Cabinet Office and the Parliamentary Security Department to issue cyber security advice, and advice on the threat from foreign interference (although the Committee did not receive any evidence as to whether that extends to advice on the vetting of Parliamentary office staff). Where necessary, MI5 also takes action to counter interference attempts. For instance, MI5 may issue Interference Alerts about individuals working on behalf of Iran (or Espionage Alerts, depending on the primary nature of the activity of individuals) to ensure that they are not able to exert influence on the UK Government.

670. The Committee was told that the Defending Democracy Taskforce is now conducting its own review into the protective security given to elected officials, which will consider "*who should receive protection; from what threats; and how this might move to be more customer-focused*".[540]

(ii) Protecting the security of UK elections

671. The Committee was told that the Defending Democracy Taskforce had established a Joint Election Security and Preparedness Unit – involving the Department for Levelling Up, Housing and Communities, and the Cabinet Office's Government Security Group – in April 2023. The Unit is working to identify and manage risks to election security and ensure preparedness ahead of the next General Election, including by working to improve HMG's response to information operations during election periods. More broadly, the Unit is working closely with NCSC to provide guidance and support to local authorities and political parties on the risk of election-related cyber-attacks.

[538] Oral evidence – Home Secretary, 6 July 2023.
[539] Written evidence – HMG, 25 August 2023.
[540] Written evidence – HMG, 13 July 2023.

(iii) Protecting the Iranian diaspora

672. The Home Office told the Committee that it had commissioned research to understand views within the Iranian diaspora, including on the Iranian regime, the threat posed and engagement with the UK Government. The research found that while many had a very negative view of the regime, very few "*were engaged with HMG in all aspects, including the police, in regard to that sort of dissident activity*". The Committee was told that this research has contributed to the Defending Democracy Taskforce's broader consideration of "*the transnational oppression that we see … and how we can get a better operational response to support diaspora communities*".[541]

The Islamic Centre of England

673. The potential role of cultural institutions in interference has been a theme in the Committee's previous Reports and, as noted in the Threat section of this Report, the Committee was told that the Islamic Centre of England (ICE) was relevant in this context.

674. The Home Office told the Committee that it recognises that it needs a greater understanding of this issue, and that it has therefore commissioned open source research to improve its understanding of the potential risks posed by ICE – *** The Committee was told that that research had demonstrated the ideology of Khomeinism promoted by ICE, and the extremist narratives that it has put across, including examples of anti-Semitism and support for the Islamic Revolutionary Guard Corps and Hizbollah. The Home Office will be using the results of that research to inform work considering the *** ICE, and the levers available to counter them. For example, the Home Office is exploring a variety of routes to determine viable and proportionate action, including *** (although the Committee was not provided with any detail on how these powers might be used); the Charity Commission is also undertaking a statutory inquiry into ICE over serious governance concerns and recently appointed an individual to take over the running of the centre (although at the time of writing, the mosque had been closed down temporarily due to an inability to obtain buildings insurance).

675. When the Committee questioned the Home Secretary as to what action was being taken, she told us that individuals who have ***, ensuring a much greater level of monitoring and control over ***. HSG told the Committee that it was "*looking as hard as we possibly can at any transgression they may have done and looking at all the possible levers across government that we might be able to pull to take action against them*".[542]

Countering online disinformation

676. The Deputy National Security Adviser (DNSA) told the Committee that the Counter Disinformation Cell – part of the Department for Science, Innovation and Technology – is responsible for monitoring disinformation activity on social media, and liaising with social media companies to illustrate where terms of service are being broken, and asking them to remove such content. However, the Integrated Review Refresh in 2023 announced the establishment of a new Government Information Cell, based in the Foreign, Commonwealth

[541] Oral evidence – HSG, 21 June 2023.
[542] Oral evidence – HSG, 21 June 2023.

and Development Office (FCDO), to increase capability to assess and respond to "*hostile manipulation of information*" by actors including Iran, where this affects UK interests abroad. It is unclear to what extent its remit overlaps with that of the Counter Disinformation Cell.

677. In terms of GCHQ's activity to tackle interference and disinformation, the Committee was told that it focuses "*very much on the adversary end of that ... to identify their malicious activity such as disinformation and influence operations*". The Intelligence Community have also run operations to counter Iran's ability to spread disinformation and to interfere – such as Operation JUNIPER.

Operation JUNIPER

Operation JUNIPER was an Intelligence Community operation *** to counter Iran's ability to conduct interference operations – both in the Middle East region ***, and further afield ***. It directly supported HMG requirements ***.

Carried out in collaboration with ***, the focus of the operation ***

The operation began with ***

An extensive information operation followed to make sure the operation was known about more widely and could not be covered up by the regime, ***

HMG judges that the joint operation ***

VVVV. There are a number of boards, taskforces, working groups and reviews all working on the Government response to state interference. We question whether all are required: inevitably there will be duplication of time, effort and money. The Committee notes the tendency for there to be too many bodies co-ordinating at the expense of those bodies doing the actual front-line work.

WWWW. The Committee has yet to see the outcomes which the Defending Democracy Taskforce has been established to achieve, nor any indication that it has the authority to drive these outcomes forward across Government. It is unclear whether it truly represents a step forward in the Government's approach or simply yet another co-ordinating structure. We recommend that the Taskforce should set out its objectives and achievements in an annual statement to Parliament.

XXXX. Work to tackle disinformation and work to protect the security of the UK's democratic processes is clearly linked. The Committee considers that Parliament should be provided with a clear statement as to the work that will be completed ahead of the next General Election, with the associated classified material being provided to this Committee.

YYYY. The Committee recommends that the Government strengthen guidance to Parliament on vetting of staff employed in MPs' offices, in the context of recent high-profile allegations of espionage carried out by Parliamentary staffers.

ZZZZ. Whilst we are reassured that the Home Office is now investigating the threat posed by Iranian-aligned cultural groups – particularly the Islamic Centre of England – it is important that the Home Office's research is followed up with specific and timely action to ensure any threat from radicalisation, promotion of extremist material, and intimidation of UK-based students and diaspora is addressed.

THE RESPONSE: NUCLEAR PROGRAMME

678. Iran's nuclear programme presents one of the most important – and challenging – aspects of the Government's response to the Iranian threat. Presuming that defending its nuclear programme will be a priority for Iran, it would therefore present a challenging target for the UK Intelligence Community. The Chief of SIS explained:

> ****, people expect foreign intelligence services to go after their nuclear programme ***.*[543]

679. The Committee was provided with examples of the agreed policy outcomes against which the UK Intelligence Community must deliver intelligence to support HMG's understanding in relation to the nuclear issue. These include:

- contribute to HMG's understanding of *** in order to inform policy;
- strengthen *** that can support HMG policy; and
- understand *** to inform HMG policy, and ***
- understand *** – to inform UK policy; and
- support *** to protect UK interests.

680. As explained previously, DI is tasked separately to GCHQ and SIS. It provides all-source assessment on Iran's nuclear *** nuclear capabilities. DI's work on the Iranian nuclear programme includes:

- assessing overt nuclear programme activity, including compliance and non-compliance with the Joint Comprehensive Plan of Action (JCPOA) ***;
- assessing the potential timelines for Iran to produce fissile material for nuclear weapons and/or develop nuclear weapons;
- assessing the proliferation risks ***; and
- engaging with international partners on the Iran nuclear issue.

Counter-proliferation: Iran's declared nuclear activities

681. Intelligence is provided on ***, including *** relating to ***. The Committee was told that the Intelligence Community also draw on expertise *** understand Iranian-declared nuclear activities: "*in this area *** people … who have a deep knowledge of the nuclear issue, ****".[544]

682. The Intelligence Community also share some of their sovereign capabilities with international partners to support understanding of Iran's declared nuclear activity. For instance, GCHQ shares a range of techniques, technology and expertise with partners, which

[543] Oral evidence – SIS, *** June 2023.

[544] Oral evidence – ***, *** June 2023.

is particularly valuable for those partners which are not nuclear states. In return, the Intelligence Community receive information which complements the UK's coverage and informs HMG's understanding of Iran's declared nuclear activity.[545]

Counter-proliferation: holding Iran to account

683. The Intelligence Community's work is also vital for HMG's efforts to hold Iran to account for its nuclear activities. When the UN's International Atomic Energy Agency (IAEA) revealed the existence of Iran's undeclared uranium enrichment programme in 2003, ***. Despite Iranian claims that the programme had been formally closed down, in 2009, the UK, US and France publicly announced the existence of a further undeclared Iranian nuclear facility at Fordow. Following this announcement, HMG was closely involved in an intelligence diplomacy campaign "*to bring a continued awareness to the international community about Iran's nuclear programme*".[546] *** HMG shared intelligence with key interlocutors ***. This intelligence diplomacy was described by HMG as one of the greatest successes ***.

684. HMG has also maintained a longstanding relationship with ***, and has briefed ***. HMG described this as: "***".[547]

685. Given the importance of the Intelligence Community's contribution to HMG's understanding of any nuclear activity by Iran, the Committee was concerned to hear doubts expressed by some of our External Experts as to whether HMG and the international community understand activity at Iran's undeclared sites. Dr Vakil recommended "*further intelligence fact-finding and gathering, access to the unknown facilities that have not been seen, where there is no oversight*",[548] and Ambassador Bolton similarly recommended it be a priority to "*get access to the military facilities and find out what is actually going on*", given that the IAEA's access to Iranian nuclear sites under the provisions of the JCPOA has been increasingly chipped away at by Iran. Ambassador Bolton emphasised the benefits that such classified intelligence would bring for the IAEA: were the IAEA to receive "*information from intelligence services of* [UN] *member states* ... [then it could act on that] *but when it is given a particular assignment, all it can do is carry out the monitoring of what is in front of it*".[549] However, when we put this to the JIC Chair, he told the Committee that while there is a risk of a "*grandmother's footsteps*" effect (in which Iran incrementally mastered different areas of technology which it was then able to apply in combination to develop a nuclear weapon), ***.[550]

[545] Quarterly Report – SIS, October–December 2016.

[546] Written evidence – HMG, 13 July 2023.

[547] Oral evidence – HMG, *** June 2022.

[548] Oral evidence – Dr Sanam Vakil, 21 March 2023.

[549] Oral evidence – Ambassador John Bolton, 21 March 2023.

[550] Oral evidence – JIO, *** June 2023.

Counter-proliferation: understanding weaponisation plans and countering progress

686. As referenced in the Threat section of this Report, the Intelligence Community have "*** *weaponisation*" and "*** *the initial stages of weapons development*".[551] The JIO noted how the evolution of Iran's nuclear programme had affected this:

> *we always had *** with regard to fissile material ... HMG had information *** from the* [publicly available] *IAEA reports on what they are up to.* [However] *as we get further on ... fissile material is not really a ... constraint in the way it was a few years ago.*[552]

687. As a result, the JIO's confidence and ability ***.[553] GCHQ explained to the Committee that *** was therefore a priority across the entire Intelligence Community and that it has dedicated additional resources to ***. These additional resources include linguists and analysts focused on *** – efforts which the Committee was told have "*led to modest success thus far*". Nevertheless, GCHQ was clear that:

> ***.[554]

688. The Foreign Secretary told the Committee that this work was "*inherently difficult*" and "*an area of work *** is absolutely key*". He told us that he had received intelligence ***, which he was able to discuss with his *** counterparts, and said that the level of insight he received was ***.[555]

689. The Committee asked the Intelligence Community whether there was any action to disrupt or counter any progress on Iran's nuclear programme, having noted previously in this Report that *** Iran ***. GCHQ told the Committee that the Intelligence Community's ***. The Chief of SIS agreed, telling the Committee that ***.[556]

690. Overall, while the Committee was provided with a good level of detail as to HMG's use of intelligence diplomacy, and the Agencies' coverage work, we received less detail on ***. Nevertheless, we were provided with detail of activity – including to ***. One such case was Operation KOKUM.

Operation KOKUM

***

[551] Oral evidence – JIO, *** June 2023.
[552] Oral evidence – JIO, *** June 2023.
[553] Oral evidence – JIO, *** June 2023.
[554] Oral evidence – GCHQ, *** June 2023.
[555] Oral evidence – Foreign Secretary, 6 July 2023.
[556] Oral evidence – SIS, *** June 2023.

691. When the Committee asked GCHQ for examples of any *** work against the Iranian nuclear programme, GCHQ told us that there was:

> ***.[557]

According to media reporting, Israel has conducted covert operations to disrupt Iran's nuclear programme. For example, it is widely reported that the Stuxnet cyber-attack (revealed in 2010) was jointly developed and co-ordinated by Israel and the US National Security Agency – although this has not been formally acknowledged.[558] Media reporting claimed that up to 1,000 of Iran's centrifuges were destroyed by this malware.[559] More recently, in 2020, Iran blamed Israel for the assassination of its senior military nuclear official, Mohsen Fakhrizadeh,[560] and attributed an explosion at Iran's Natanz facility in December 2021, which set its nuclear programme back by months, to Mossad.[561]

692. We asked whether the National Cyber Force (NCF) had conducted operations to disrupt Iran's nuclear programme. The Chief of Defence Intelligence (CDI) told the Committee that this was "*** *I don't think there is much active NCF operation at the moment on* ***".[562] GCHQ elaborated that: "*in terms of offensive cyber operations delivered by NCF,* *** *is not at the moment one of the most active ones, but they are scoping out options for that*". We were told that the current priorities for NCF's effects work against Iran related to ***.[563]

693. DI told the Committee that it had undertaken support work for *** Iran's nuclear programme – for instance, DI had provided intelligence assessments and expert advice on ***.

A new settlement: understanding and discouraging

694. As we note above,[564] it appears that Iran has not yet taken the decision to weaponise its nuclear programme. The Deputy National Security Adviser (DNSA) told us that HMG was working to "*maintain a credible pathway to stop and reverse the Iranian nuclear programme and, obviously, we are working very closely with US and E3 partners in order to do that*".[565]

695. GCHQ and SIS ensure that Whitehall policy teams are kept informed of the latest intelligence, and that they in turn adapt their intelligence-gathering efforts to meet policy-makers' requirements. DI provides all-source assessment to keep policy teams up to date with developments. During the JCPOA negotiations, *** informing the delegation's approach

[557] Oral evidence – GCHQ, *** June 2023.
[558] 'Stuxnet Was Work of U.S. and Israeli Experts, Officials Say', *The Washington Post*, 2 June 2012.
[559] It was reported in the media that this equated to approximately one in six of an estimated 6,000 Iranian centrifuges. ***
[560] 'Mohsen Fakhrizadeh: Iran Blames Israel for Killing Top Scientist', BBC News, 28 November 2020.
[561] 'Israeli Spies Tricked Iranian Scientists into Blowing Up Nuclear Plant', *The Daily Telegraph*, 2 December 2021.
[562] Oral evidence – DI, *** June 2023.
[563] Oral evidence – GCHQ, *** June 2023.
[564] At paragraph 203.
[565] Oral evidence – NSS, *** June 2023.

to negotiations. ***. Baroness Ashton told the Committee that this had provided "*a lot of useful information*" and paid tribute to the Intelligence Community's efforts.[566] This included sharing intelligence relating *** and contributing to ***.[567]

696. SIS provided intelligence to support HMG's attempts to maintain the JCPOA, and provided insight into ***.[568] For instance, SIS told the Committee in 2016 that intelligence it provided on Iranian *** gave the then FCO "*the knowledge it need*[ed] *to* ***".[569] SIS also provided reporting on Iranian efforts to *** on issues such as ***.

697. During the recertification of the JCPOA in 2017, the Intelligence Community provided intelligence that allowed the National Security Adviser to challenge *** understanding of Iran's ***. Insight was provided into Iranian *** the nuclear deal, which supported HMG's engagement with *** by highlighting Iran's adherence to its JCPOA obligations. In 2018, insight was also provided on likely Iranian ***.[570]

698. More recently, GCHQ intelligence has provided detailed insight into Iranian ***. For example, GCHQ reporting showed Iran's *** and, following the US withdrawal from the JCPOA, intelligence indicated Iranian ***. GCHQ and DI also look for ***.

699. Following the US withdrawal from the JCPOA, and after formal negotiations to return to the JCPOA began in 2021, GCHQ and SIS provided reporting on ***, including:

***

The Committee was told that these insights *** directly informed the tactics and policies pursued by HMG, giving it ***. GCHQ told us that it also ***.[571]

700. DI has provided the Foreign, Commonwealth and Development Office (FCDO) and the Ministry of Defence (MoD) with intelligence assessments and expert advice on the likely impact of proposed agreements to limit Iran's nuclear programme. In evidence to the Committee's International Partnerships Inquiry, the CDI described DI's experts *** as "*absolutely world-leading*" and recognised as such by allies.[572] MI5 also "*supports HMG when considering the likely retaliatory actions that Iran might take under different scenarios relating to the collapse of the negotiations*" – a scenario which appears to have now materialised. This includes what impact those actions would have on the threat Iran poses to the UK and to UK interests in the region.

Monitoring effectiveness of sanctions

701. It appeared that HMG accorded a lower priority to monitoring sanctions compliance ***. We were told that ***

[566] Oral evidence – Baroness Ashton, 21 March 2023.
[567] Quarterly Report – SIS, October–December 2017.
[568] Quarterly Report – SIS, July–September 2018; Quarterly Report – SIS, January–March 2019.
[569] Quarterly Report – SIS, July–September 2016.
[570] Quarterly Report – SIS, January–March 2018.
[571] Oral evidence – GCHQ, *** June 2023.
[572] Oral evidence (International Partnerships Inquiry) – DI, *** June 2021.

702. HMG has also received reporting on the state of Iran's economy, and on Iranian efforts to evade international sanctions and build a 'resistance' economy. Reporting has shed light on Iran's desire to develop multilateral economic relations with countries in the Middle East and with China, in order to reduce the effect of sanctions. Intelligence has also indicated that ***.

AAAAA. We recognise that the Iranian nuclear programme, though one of the most difficult elements of work on Iran, is also the most important.

BBBBB. The Community have * in their understanding of *** weaponisation and *** the initial stages of weapons development. The UK – and perhaps the rest of the international community – may therefore have *** notice period before Iran is able to conduct a nuclear weapons test. *** is a priority across the entire Intelligence Community.**

CCCCC. GCHQ and SIS reporting has provided crucial insights into *, directly informing the tactics and policies pursued by HMG: their continuing insight is essential as the UK seeks to discourage Iranian nuclear escalation.**

DDDDD. The Intelligence Community seeks * Iran's nuclear programme ***. While we appreciate that such activity is difficult, and must be carefully considered, we found this surprising because of the *** priority given to Iran's nuclear programme in the National Security Council Iran Strategy.**

703. As noted previously, the UK has substantial security and commercial interests in the Middle East which are at risk from Iranian hostile activity. There is a threat to individuals (whether a specific threat to UK–Iran dual nationals, or to staff working at the British Embassy in Tehran, or a general threat from a ballistic missile attack or a chemical weapons attack) and a threat to the UK's maritime, commercial, energy and security interests.

704. While we explore the action being taken to address these issues below, it is worth noting that should the situation in, or relationship with, Iran deteriorate quickly, there could be a need to evacuate UK nationals rapidly – and we therefore note the failures in relation to the withdrawal from Afghanistan, for example. The Committee questioned the Foreign Secretary as to whether the UK is more prepared in the case of Iran. The Foreign Secretary told the Committee: "*we don't know exactly how many British nationals are in the region or how many would want to be supported in case of escalation*"[573] – explaining that while there are a significant number of UK nationals in the region, it is not mandatory for these individuals to register with the Foreign, Commonwealth and Development Office (FCDO).

705. The Foreign Secretary was, however, clearly mindful of the risk – acknowledging that "*an evacuation response would be a very, very significant and challenging operation*".[574] Perhaps for this reason, he described the UK's approach to managing the threat to UK individuals and interests in the region as being to "*deter and defend*".[575]

Individuals

706. We noted earlier in the Report the significant threat to UK nationals in the region. In terms of the risk to UK–Iran dual nationals, our External Experts were clear that HMG was not doing enough in terms of deterring individuals from travelling:

> *There needs to be much clearer advice going out on the Foreign Office website and elsewhere that, you know, this is a threatening journey, don't make it if you don't have to. It is kind of like an amber weather warning: if you don't have to go there, don't do it. That message needs to get across much more clearly.*[576]

707. However, when we put this to the Foreign Secretary, he told the Committee that in his view HMG was "*pretty explicit in the travel advice, which is: you shouldn't go there; if you do go there, we cannot help you*" – noting that at the end of the day HMG could not mandate that individuals follow the travel advice.[577] The Committee asked the Intelligence Community whether more robust advice – or more active messaging targeted at specific groups – might help reduce the threat from Iran to dual nationals. MI5 – which works in conjunction with UK and international partners to identify and counter threats to UK nationals in the region –

[573] Oral evidence – Foreign Secretary, 6 July 2023.
[574] Oral evidence – Foreign Secretary, 6 July 2023.
[575] Oral evidence – Foreign Secretary, 6 July 2023.
[576] Oral evidence – Professor Anoush Ehteshami, 9 March 2023.
[577] Oral evidence – Foreign Secretary, 6 July 2023.

told the Committee that it would be "*difficult*" to take a more active approach to spreading the message in the Middle East, noting that this lay firmly with the FCDO: "*for people in the region, or in Iran, that is through the country guidance that the Foreign Office issue. There are not really other channels to do that*".[578]

708. When Iran has detained UK nationals, the *** has supported the Government's response ***. The Foreign Secretary told the Committee that during negotiations to repatriate ***. He told the Committee that this had "*helped enormously* ***".[579] As a result, HMG was able to secure the release of the detainees concerned.

709. MI5 and DI also support the Government's response to cases where dual nationals have been detained by a foreign state: MI5 provides an investigative response to assist policy departments in identifying when a dual national has been detained *** and advises on potential operational responses, while DI produces relevant assessments ***.

710. The HMG staff based at the Embassy in Tehran are also at risk. HMG emphasised the value of the diplomatic presence; as the Deputy National Security Adviser (DNSA) said, "*the fact that ... we continue to have that Embassy provides us with an* [diplomatic] *advantage which ...* [others] *don't necessarily have*". However, that comes with risk attached in terms of the threat to staff working in the Embassy – albeit one that can be a challenge to understand, as outlined in the Threat section. The Foreign Secretary told the Committee:

> *We do consider the protection of our staff ... we do have a duty to our staff to protect them. *** in terms of losing access to that* [diplomatic] *platform, but we do recognise that ... that is something we have to keep under constant consideration.*[580]

The Committee notes the importance of proper preparation for a possible evacuation. ***

UK interests

711. UK interests in the region – whether commercial or military – are at risk from attacks – for example, from ballistic missiles or Chemical and Biological Weapons (CBW), as described in the Threat section of this Report. In terms of the threat from CBW, the Committee was told that ***[581] ***.[582]

712. The Foreign Secretary acknowledged that *** – but he reassured the Committee that he was "*conscious*" of the issue and recognised that "*I think we will need to do more, as the risk involved evolves*".[583]

713. In terms of the threat from Iran's *** ballistic missile programme, the Committee was told that although historically the Intelligence Community had sought coverage of *** –

[578] Oral evidence – MI5, *** June 2023.
[579] Oral evidence – Foreign Secretary, 6 July 2023.
[580] Oral evidence – Foreign Secretary, 6 July 2023.
[581] Oral evidence – ***, *** June 2023.
[582] Written evidence – HMG, 21 April 2022.
[583] Oral evidence – Foreign Secretary, 6 July 2023.

primarily to identify "***"[584] – more generally the Intelligence Community had "***",[585] which was ***. (The Intelligence Community told the Committee that they had previously monitored *** in order to identify where technology is being developed which could be applied to the development of ***.)

714. The Committee was subsequently told in 2023 that *** Iran's ballistic missile programme was increasingly important *** given the substantial improvement in Iran's ballistic missile capability in recent years.[586] When the Committee asked whether the Intelligence Community were confident that they could detect a further increase in Iranian ballistic missile capability, the Intelligence Community said that they had *** the Intelligence Community noted that they were not expecting ***.[587]

715. From the evidence we received, it appeared that *** to the Iranian maritime threat in the Gulf (***). For instance, *** Iranian naval activity in the Gulf, ***.[588] As a result, it appeared that ***.[589] The response to Iran's 2021 attack on the *MV Mercer Street* tanker in international waters – detailed in the Threat section – demonstrated ***. On that occasion, the UK was able quickly to attribute the attack to Iran ***. A form of words was provided to international partners, and this resulted in a statement from the G7 regarding Iranian culpability.

716. In terms of the military aspect, DI told the Committee that "*the UK–Iran defence relationship is fairly predictable and stable, but of course that can change quickly, when Israel or the US end up in exchanges with Iranian military, which then can draw in the UK* ***".[590] We were reassured, however, to hear that the National Security Secretariat was working on contingency planning around potential military escalation in the region, looking at how the UK would respond in legal, military and diplomatic terms.

Aligned militant and terrorist groups

717. The Foreign Secretary told the Committee that the National Security Council (NSC) had identified understanding Iran's malign regional activity – including its provision of support to a network of aligned militant and terrorist groups across the region – as a priority.

718. Under the tri-Agency 'Iran Mission', the Agencies structure their response to the threat posed by Iranian-aligned groups to UK interests in the region – as well as the threat these groups pose to the UK itself – around the following areas:

***

[584] Oral evidence – ***, *** June 2023.

[585] Written evidence – HMG, 21 April 2022.

[586] 'Table of Iran's Missile Arsenal', Iran Watch, 22 February 2024; 'UK Statement at Conference on Disarmament: High Level Segment', FCDO, 28 February 2024.

[587] Oral evidence – ***, *** June 2023.

[588] Oral evidence – ***, *** June 2023.

[589] Oral evidence – ***, *** June 2023.

[590] Oral evidence – DI, *** June 2023.

719. In ***, MI5 *** the relationship between Iran and its regional proxies (***), so that ***.

720. ***. As part of this, MI5 created a new team to work on Iran's use of 'partner and proxy' groups based in the Middle East, and the threat of terrorist activity by these groups against both the UK and UK interests in the region. An initial priority for this work was Lebanese Hizbollah – including insight into its activities and intent in the UK. Since ***, MI5 has *** Iranian lethal threat operations targeting UK-based individuals. The 'partner and proxy' team also investigated the Iranian Intelligence Services' (IIS's) relationship with ***. HMG told the Committee that it considered the close working between the MI5 'partner and proxy' team and the joint *** team that focuses on *** to have been vital in ***.

721. SIS and GCHQ told the Committee that they devote *** resource to providing intelligence coverage of the *** proxies which are judged to present the greatest threat to the UK and its interests. GCHQ told the Committee that it ***.[591] The Chief of SIS told the Committee that his agency had ***.[592] SIS told us that its work on *** received a higher priority than other Iranian proxies: "*there is threat to us clearly and that does manifest itself, including in the loss ***. So we would definitely try harder to focus on that ... with ***, there is not a direct threat in the same way, so it wouldn't be the priority.*"[593] Nevertheless, the Committee was provided with some examples of successful SIS operations ***, as detailed in the box on Countering activity below.

722. In terms of Afghanistan, *** to HMG's understanding of Iran's support for Al-Qaeda in Afghanistan, and – until the withdrawal of UK personnel from Afghanistan in August 2021 – MI5 also investigated *** where this relationship was assessed to increase the threat to UK interests in Afghanistan. GCHQ provided insights into the threat from Iranian proxies *** – such as *** and the threat they pose to HMG interests ***, which directly informed HMG's response during the 2021 withdrawal from Afghanistan.

Countering activity

In *** HMG conducted a range of initiatives to counter Iranian malign activity in the region, focused on ***. Through Operation TURMERIC, SIS collected intelligence ***.

SIS ran an operation to disrupt ***. SIS worked with the FCDO to deliver a disruptive briefing to ***, and the Chief of SIS described this operation as achieving "***".[594]

723. SIS told the Committee that it no longer ***. This decision was made "*on the basis of resource expenditure against relative impact of SIS actions*". When we questioned the Chief of SIS about this, he told the Committee that this was "*purely a question of resourcing and the effectiveness of* ***".[595]

[591] Oral evidence – GCHQ, *** June 2023.

[592] Oral evidence – SIS, *** June 2023.

[593] Oral evidence – SIS, *** June 2023.

[594] Oral evidence – SIS, *** June 2023.

[595] Oral evidence – SIS, *** June 2023.

Iranian use of criminal groups as proxies

724. MI5 told the Committee that "*** *the criminal groups that they are using, which is very disparate, and we are working quite hard with CT Policing partners and the National Crime Agency* *** *to disrupt them*."[596] MI5 is seeking now to *** those criminal groups – including drug smuggling networks and crime groups – and is working with *** to disrupt some of those networks. MI5 considered this to be "*a really challenging thing, given the breadth of actors that they are willing to use but that is something we are really focusing on with our operational partners here and internationally*".[597]

EEEEE. Given the volatility of the situation, the potential for misunderstanding and miscalculation by Iran, and the possibility for rapid escalation, it is not unrealistic to think that at some point it could become necessary to evacuate UK nationals in the region. The Committee notes the importance of proper preparation for a possible evacuation. * the Government must ensure that it has learnt the lessons from recent evacuation operations such as the withdrawal from Afghanistan.**

FFFFF. We note that work to * and are reassured that ***.**

GGGGG. The Government should use all the tools at its disposal to degrade the relationship between Iran and groups such as Al-Qaeda and Lebanese Hizbollah, including publicly calling out Iran's attempts to protect such terrorist groups.

[596] Oral evidence – MI5, *** June 2023.

[597] Oral evidence – MI5, *** June 2023.

ANNEX A: FULL LIST OF RECOMMENDATIONS AND CONCLUSIONS

A. The foundation of the Islamic Republic of Iran in 1979 was a pivotal moment in Iranian history as it moved from an absolute monarchy to a partial theocracy, ruled by the Shi'a clergy.

B. The Supreme Leader of Iran wields tremendous power – he is the ultimate decision-maker, setting the direction of Iranian foreign and domestic policy. In terms of the threat posed by Iran to the UK and its interests, the Supreme Leader is therefore key.

C. The Iranian threat appears to have increased following the election of Ebrahim Raisi as President, who is more ideologically aligned with the Supreme Leader than his predecessor. This means the regime may act in a more provocative manner with less restraint.

D. The organisations within the Iranian Intelligence Services – primarily the Ministry of Intelligence and Security and the Islamic Revolutionary Guard Corps, representing the republican and revolutionary organs of state – have overlapping remits, which results in fierce competition, tension and disagreement. Whilst the Iranian Intelligence Services operate within a general framework, it appears there is still a certain level of autonomy. Activity may therefore not always be effectively co-ordinated nor centrally authorised.

E. The Committee considers that the relative autonomy of, and factionalism within, the Iranian Intelligence Services increase the risk of unmanaged escalation and contribute to a worrying unpredictability around the Iranian threat to the UK and UK interests in the Middle East. However, increased co-operation and capability-sharing within the Iranian Intelligence Services could also raise the Iranian threat.

F. The Iranian regime's fundamental objective is to ensure the survival and security of the Islamic Republic: it has an acute historical sense of vulnerability. This shapes – directly or indirectly – all of its actions. This focus on survival means Iran is a pragmatic actor, often driven more by opportunism than ideology (more 'securitocracy' than theocracy).

G. The Iranian regime has three key regional aims: to be a leading regional power; to contain perceived US and Western influence and hostility; and to protect Shi'a communities and holy sites.

H. Whilst Iran favours proportionality in relation to conflict, this is not always achievable or pragmatic as it wants to avoid a full-scale war. It therefore has focused on the development of 'asymmetric' capabilities and a network of aligned militant and terrorist organisations across the Middle East to spread influence and deter potential aggressors.

I. Iran also maintains a fierce ideological, religion-based hostility to Israel, regarding it as its arch enemy. The Supreme Leader is so wedded to this narrative – from the Revolution – that it is now part of the Iranian regime's DNA.

J. Iran is motivated by both defensive and offensive considerations. Much of Iran's foreign policy – and the threat it represents to the UK – is borne of a historical sense of its regional importance, a fear of encirclement by better-equipped Western adversaries, a history of perceived foreign interference in Iran, and the formative experience of the Iran–Iraq War.

K. While Iran is fundamentally a rational actor, it does not always appear to act in a coherent way and is prone to misunderstanding actions that others take.

L. Iran and the UK have a complex history. Iran's leadership perceives the UK to be a significant adversary – a 'cunning fox' – opposed to the Iranian regime's values and, as part of the West, to be seeking regime change in Iran. It therefore believes that the UK poses a military and intelligence threat in the Middle East – although witnesses suggested that the UK would sit behind the US, Israel and Saudi Arabia in any priority list.

M. Iran's main strategic objectives towards the UK include: reducing the UK's military presence in the region; undermining the UK's relationships with the US and Israel; weakening the UK's security relationships in the Middle East; and silencing criticism of Iran, either from the UK directly or from those residing in the UK.

N. The threat posed by Iran is also linked to the state of the bilateral relationship between Iran and the UK. This relationship could change depending on the UK's international engagement as much as UK-specific actions or policy. The Intelligence Community also noted that Iran's approach towards the UK is closely linked to its approach to the US – unsurprising given the close alignment between the UK and the US.

O. Whilst Iran's activity appears to be less strategic and on a smaller scale than Russia and China, Iran poses a wide-ranging, persistent and sophisticated threat to UK national security, which should not be underestimated.

P. Iran's acute sense of its position in the region – including its perceived vulnerability – drives its strategy towards its international partnerships.

Q. Iran wants to build a deep alliance with Russia, and the relationship is becoming increasingly close – despite a legacy of distrust and suspicion – particularly since the Russian invasion of Ukraine, with Iran providing weaponry to Russia. The relationship is driven by political expediency rather than ideological connection. It appears likely that their intelligence services co-operate and share intelligence.

R. China is Iran's largest trade and economic partner, and they share a world view driven by preserving regime legitimacy, a sense of grievance in relation to past foreign interference, and a suspicion of the West. Whilst there may well be intelligence exchanges between the two countries, the intelligence relationship is probably of less significance than the economic relationship.

S. Iran has developed a network of complex relationships with militant and terrorist groups across the Middle East to which it provides differing levels and types of support. It maintains these relationships through both the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security, but particularly the IRGC Quds Force, which provides training, lethal aid, funding and, in some cases, direction to these groups. This network is part of Iran's doctrine of 'strategic depth', ensuring that it does not enter into conflict with superior conventional powers within its own borders. It provides Iran with a deniable means of threatening its adversaries – such as UK Armed Forces and the UK's regional allies – and undermining Western interests in the region with minimal risk of retaliation against Iranian territory.

T. The varying level of control that Iran exercises over its network of aligned militant and terrorist groups – and the different interests represented within it – exacerbates the unpredictability of the Iranian-backed threat in the Middle East and risks an escalation of aggression in the region.

U. The transactional arrangement between Iran and the senior leadership of Al-Qaeda (AQ) is concerning. Being based in Iran has allowed AQ to retain some oversight of franchises internationally, creating a complex intelligence landscape, as Iran is a less accessible environment for the West than other parts of the Middle East – which, in turn, may have increased the AQ threat.

V. There has been a significant increase over the last 18 months in the physical threat posed by Iran to those residing in the UK. There have been at least 15 attempts at murder or kidnap against British nationals or UK-based individuals since the beginning of 2022. The threat of physical attack on individuals in the UK is currently the greatest threat we face from Iran and is now on a broadly comparable level with Russia.

W. The Iranian physical threat in the UK is focused acutely on dissidents and other opponents of the regime. The targeting of dissidents is one of the Iranian Intelligence Services' highest priorities, and Iran is prepared to assassinate dissidents in the UK.

X. Iran does not view attacks on dissident, Jewish and Israeli targets in the UK as attacks on the UK. It rather sees the UK as collateral in its handling of internal matters – i.e. removing perceived enemies of the regime – on UK soil.

Y. The Iranian Intelligence Services have shown that they are willing and able – often through third-party agents – to attempt assassination within the UK, and kidnap from the UK, although in respect of the latter they prefer to lure individuals * to a third country in which the Iranian Intelligence Services can operate more easily, and forcibly repatriate them from there.**

Z. The Iranian Intelligence Services are increasingly using organised criminal gangs to undertake hostile activity abroad. Some of the criminal groups used by Iran to conduct operational activity have links to Russia. The use of such gangs provides deniability for Iran. In addition, the wide range of organisations used means a broad pool of suspects – adding a further layer of unpredictability.

AA. Nuclear proliferation around the world, including in the Middle East, is a critical threat to the UK on a number of levels. Iran proceeding with its nuclear weapons programme therefore poses a threat both to UK nationals in the region and to the UK mainland – and to global security more broadly if it led to regional nuclear proliferation and exacerbated regional instability.

BB. It appears that Iran has not yet developed a nuclear weapon nor taken a decision to produce one, but it maintains the option of developing one – largely as the 'ultimate security guarantee'. It is difficult to determine what would trigger such a decision by the Supreme Leader: it is plausible that Iran's intent is to maintain a state of 'nuclear ambiguity' at the threshold of weaponisation; however, it may choose to weaponise if it feels it is facing an existential threat.

CC. Whilst the 2015 Joint Comprehensive Plan of Action nuclear agreement had its limitations, the Intelligence Community believes that – before the US's withdrawal in 2018 – Iran was broadly compliant with the restrictions on its nuclear programme; this appears to have reduced the Iranian nuclear threat, if only in the short term.

DD. Since the US's withdrawal from the Joint Comprehensive Plan of Action, the Iranian nuclear threat has increased as Iran has taken steps in developing its nuclear programme. While it appears that it is still short of the 'weaponisation' phase, the potential timelines have reduced over the last few years and Iran has the capability to arm in a relatively short period – possibly * to produce a testable device and *** to develop a deliverable nuclear weapon.**

EE. Given the increase in the Iranian nuclear threat, negotiating a form of de-escalation between Iran and the international community must be a priority. This may be a limited successor to the Joint Comprehensive Plan of Action, a broader multilateral agreement dealing with regional security or separate bilateral agreements with Iran: all would serve to reduce the current high tension.

FF. Iran poses a significant espionage threat to the UK and its interests, projected primarily via cyber capabilities, but also via human agents. Whilst as a target, the UK appears to remain just below the US, Israel and Saudi Arabia, this prioritisation could change depending on geopolitical developments and the relationship between Iran and the UK.

GG. The espionage threat is focused on supporting Iran's primary objective of regime stability: it is substantially narrower in scope and scale, and less sophisticated, than that posed by Russia and China. In the UK, the Iranian Intelligence Services prioritise targeting opponents of the regime, HMG and sectors that may provide the Iranian regime with a strategic advantage such as academia and defence. However, the Iranian espionage threat may not necessarily follow a set strategic plan – there is more of an opportunistic element in its targeting.

HH. There is a collateral threat to the UK associated with Iran's targeting of regional networks and multilateral organisations. Given Iran's focus on the Middle East, Iranian cyber actors in the region are particularly active. This increases the risk to the UK if it were to share sensitive data with those whose networks may be a target of the Iranian Intelligence Services.

II. While both the Iranian Embassy and the Islamic Centre of England have legitimate roles supporting the Iranian diaspora community, given their close links to the Iranian regime they are also likely to provide a permissive environment for Iranian Intelligence Services agent recruitment and intelligence gathering in the UK. We encourage the Intelligence Community not to underestimate the potential espionage threat they pose.

JJ. Iran is an aggressive cyber actor with extensive capabilities. Whilst Iran does not possess the same sophisticated capability as Russia and China, the cyber threat posed by Iran is significant.

KK. The Iranian cyber threat landscape is complex, with cyber groups ranging from state-controlled actors responding to direct tasking, to private cyber actors working for personal gain or perceived state intelligence requirements. The complexity of this environment appears to make it more difficult to identify accurately the motivation behind Iranian cyber activity and the level of state control.

LL. Whilst Iranian cyber actors often use simple computer network exploitation techniques, they use them very effectively, exploiting basic vulnerabilities that many organisations have, including in the UK. They do this for the purpose of gathering intelligence, undertaking interference operations and enabling offensive (disruptive and destructive) cyber operations.

MM. The ever-increasing interconnectivity of global technology and developments in Artificial Intelligence may exacerbate the Iranian cyber threat.

NN. Iran generally favours proportionality, responding in a similar way to perceived aggression. Where that is not achievable or realistic, it uses asymmetric capabilities – of which offensive cyber is a prime example.

OO. Offensive cyber – by which we mean both destructive and disruptive cyber-attacks – allows Iran to attack and contain Western and regional adversaries without resorting to conventional military action. It also provides Iran with a deniable tool with which to attack its enemies, respond to perceived aggression and project power in the region – and globally.

PP. Although Iran does not possess the same sophisticated cyber capability as Russia and China, it is an aggressive cyber actor, with a relatively high risk appetite. However, at present, it appears that the UK is not a top priority for Iranian offensive cyber activity and, in the current environment, Iran may not attempt an offensive cyber-attack specifically to damage the UK. Nevertheless, we note that this could change rapidly in response to regional or geopolitical developments: the likelihood has increased, for example, in connection with the recent protests in Iran.

QQ. Due to multinational trade and the interconnectedness of IT networks, it is likely that any global increase in Iranian offensive cyber activity increases the risk to UK entities – for example, through collateral damage resulting from broader activity. Iran both recognises and accepts that risk.

RR. If Iran decided to conduct an offensive cyber-attack against an adversary such as the UK, the petrochemical, utilities and finance sectors could be at risk. According to the National Cyber Security Centre, it is unlikely that all UK entities are able to detect or defend against Iranian offensive cyber activity.

SS. We were told that Iranian cyber actors *. *** they could *** attempt to cause *** disruption by targeting *** Critical National Infrastructure.**

TT. Whilst ultimately unsuccessful, we noted with particular concern that Iranian cyber actors reportedly targeted water facilities in Israel. When we questioned whether the Industrial Control Systems installed in Israel are similar to that used throughout Critical National Infrastructure globally, including in the UK, we concluded *.**

UU. The Iranian regime believes it is engaged in an active information conflict with its adversaries and refers to interference activity as 'cognitive warfare'.

VV. Iran draws on the full range of state capability to conduct interference operations. This includes the Iranian Intelligence Services, state media, the Iranian Ministry of Foreign Affairs and Iranian-funded organisations. They use different platforms – both overt and covert – such as traditional media, social media and networks of purportedly 'independent' news websites, to spread their own narratives in the UK.

WW. Whilst the UK is a high priority target for Iranian interference activity due to its role in multilateral negotiations relating to Iran and the presence of several Iranian-language news outlets in the UK which are critical of the regime, it is not as important as the US, Israel, Saudi Arabia or other Middle Eastern states.

XX. Overall, HMG considers that Iran's interference operations (which seek to suppress critical voices, promote views that align with its own geopolitical narratives and religious ideology, weaken confidence in British institutions, undermine the US–UK relationship, and exacerbate wider social divides) have had a negligible effect on UK public opinion and decision-makers, including in relation to UK elections.

YY. The focus of Iran's interference operations – and of most concern – are the attempts to intimidate Iranian dissidents and those working for media organisations such as Iran International in the UK and beyond. Some reports suggest Iran's efforts to intimidate the regime's perceived opponents have had a significant impact on the Iranian diaspora community in the UK: targets of this intimidatory behaviour have limited their social contact with other Iranians, particularly those within Iran, moderated their criticism of Iran, and reduced their advocacy for contentious Iranian topics. We note and encourage ongoing efforts to support Iran International's return to the UK. However, we are concerned as to whether this means the UK is not a sufficiently hard operating environment for Iran, and whether HMG is taking sufficient proactive action to protect UK-based media organisations.

ZZ. Whilst the Islamic Centre of England and other cultural and educational centres supported by Iran have legitimate roles supporting the Iranian diaspora, there are grounds to suggest that they have been used to promote violent and extremist ideology. This threat must not be underestimated.

AAA. The UK has substantial security and commercial interests in the Middle East, which are at risk from Iranian hostile activity, including a physical threat to UK nationals in Iran, a threat to UK maritime and commercial interests in the region, and a security threat in respect of terrorism, increased migration and nuclear proliferation.

BBB. Iran has a broad range of tools it could deploy, including missiles and drones (which it could use against Israel, regional US bases – where UK forces are co-located – and Gulf energy infrastructure), its network of militant and terrorist forces, chemical weapons, offensive cyber and disruption of shipping in the Gulf.

CCC. The Iranian physical threat to UK nationals in the Middle East has increased in the last two years as a result of the internal protests in Iran. Detention remains the primary physical threat to British citizens in Iran, and is heightened in relation to dual nationals – particularly because dual nationality is not recognised by Iran. The threat of arbitrary detention has increased since the recent protests in Iran.

DDD. Whilst it appears relatively unlikely, the British Embassy in Tehran is a potential target for an attack. It may well also be the epicentre of protests in the absence of other Embassies.

EEE. The threat of collateral damage to UK Armed Forces stationed in the region (resulting from misidentification or miscalculation) is the main physical risk to British nationals in the Middle East – outside of Iran – due to their sizeable number and co-location with the more heavily targeted US forces.

FFF. In addition to launching physical or cyber-attacks on UK economic interests in the Middle East, Iran has the capability to disrupt or attack commercial shipping in the region – primarily in the Strait of Hormuz: although it practises its capability to close the Strait, it would be a major step for Iran do so.

GGG. The US killing of General Qasem Soleimani in 2020 appears to be contributing to increased regional instability. The Iranian regime may still be seeking revenge and his death * Iran's control over its network of aligned militant and terrorist groups. Given the risks of misidentification and collateral harm, we believe that this continues to pose a particular danger for UK troops co-located with US forces in the region.**

HHH. The Government's policy on Iran has suffered from a focus on crisis management, driven by concerns over Iran's nuclear programme, to the exclusion of other issues.

III. 'Fire-fighting' has prevented the Government from carrying out longer-term thinking and developing a real understanding of Iran and the complexity of the problem. The Government must stop its short-termist, reactive approach: 'longer-term' must mean the next 5, 10 and 20 years, not 6 to 12 months.

JJJ. We welcome the increased focus on Iran in the 2023 Integrated Review Refresh. However, as with our previous Inquiries into national security issues relating to China and Russia, the Government appears to over-complicate governance structures and strategies – with the attendant risk of too much talking, at the expense of action.

KKK. There is no sense from anyone we spoke to of: how the National Security Council Iran Strategy relates to the Integrated Review Middle East and North Africa sub-strategy; which of them takes precedence; and whether the National Security Council Iran Strategy has taken account of the changes in the Integrated Review Refresh. It is concerning that these strategies appear not to have been aligned.

LLL. It remains difficult to determine accountability for the National Security Council Iran Strategy – as with any strategy, it should be clear who is responsible for driving implementation, and whose performance rating and pay rewards will be determined by its success or failure.

MMM. We note with concern that the National Security Council met * to discuss Iran. If the National Security Council is to have an 'Iran Strategy', then it should be ensuring implementation of it, through regular discussions with the officials responsible.**

NNN. The Counter-State Threats Strategy has taken four years to develop – whilst this is an extraordinarily long time to wait for such a key piece of work, the Committee cannot provide Parliament or the public with any assurance that it was worth the wait: the Government failed to provide the Committee with the Strategy. We regard this as completely unacceptable: this Committee has been given the statutory responsibility to oversee such matters, and we question what the Government's reasons are for withholding it.

OOO. While we recognise that there will be some elements of the state threats from China, Russia and Iran that are broadly similar and which will benefit from an actor-agnostic approach, there will be fundamental differences which could be overlooked. The Iranian threat is quite different in many respects and it is essential that it receives sufficient priority, and that Russia and China do not dominate the Government's focus.

PPP. The Intelligence Outcomes Prioritisation Plan – which sets the requirements for GCHQ and SIS – * 'coverage' *** 'effects'. We recognise the need to prioritise *** and the relatively ***. Nevertheless, proper consideration must be given to ***.**

QQQ. It is a step in the right direction that the Intelligence Outcomes Prioritisation Plan in 2022 introduced a requirement to provide greater understanding of Iran's *.**

RRR. We are concerned by the lack of engagement between the Foreign Secretary and his Iranian counterpart; Ministerial channels can be useful in delivering messaging to deter malign activity, and to reduce the risk of misunderstanding and unintended escalation.

SSS. We are surprised at the relative infrequency of meetings between the Foreign Secretary and the Heads of GCHQ and SIS, compared to the greater engagement by previous Foreign Secretaries.

TTT. Resourcing on Iran has fluctuated over the past decade, supporting the concern that the response to the Iranian threat has been short-termist. * resourcing did not then increase following *** – given that Iran has consistently reduced its compliance since then.**

UUU. We have previously made reference to the fact that the Agencies do not have unlimited resources, and therefore hard choices on resourcing and prioritisation must be made during national security crises. It is clear to us that the situation during the conflict in Ukraine, for example, is no different.

VVV. GCHQ in particular recognises that its drawdown in resourcing * had significantly affected *** While GCHQ argued that it was doing 'more for less', this is nevertheless concerning.**

WWW. MI5 has still not been given the additional funding and resources that we called for in our *Extreme Right-Wing Terrorism* Report. Without a commensurate increase in resources, MI5 cannot be expected to absorb responsibility for an increased range of issues, without other areas of work suffering as a consequence.

XXX. Across Government, there is a lack of Iran-specific expertise and seemingly no interest in building a future pipeline of specialists, beyond mention in a Strategy campaign. We were particularly struck by the critique, "*if you have people running policy in the Foreign Office who don't speak a word of Persian, then that is a fat lot of good, to be honest*".

YYY. The Government's response to the Iranian threat appears to be wrapped up with state threats or the Middle East. This may be positive if it means that Iran will benefit from synergies with work to counter other – perhaps more prominent – state threats. However, the risk is that this instead results in a less tailored and therefore less effective response to the Iranian threat.

ZZZ. The Agencies' partnerships with the US * on the Iranian threat are of critical importance, and the *** countries operate with an exceptionally high level of trust.**

AAAA. The Agencies' close collaboration with the US and other international partners in relation to the Iran threat appears to be one of their greatest assets: it yields great value and lessens burdens. However, it also appears to be a potential vulnerability, in that if this arrangement were to cease, it is doubtful whether the Intelligence Community would be able to respond to the Iranian threat anywhere near as effectively.

BBBB. Most countries – even our closest allies – will operate under different legal and ethical constraints to the UK. However, to protect the UK we have no choice but to work with other countries. The framework under which our Agencies engage is therefore of the utmost importance. The evidence we have received reassures us that where HMG engages in a joint operation, UK 'red lines' are made clear to ensure that legal and policy boundaries are observed and that, wherever possible, appropriate due diligence is carried out to ensure that information is not obtained via prohibited methods. However, we note that that cannot be guaranteed.

CCCC. We recognise the benefits of sharing intelligence *. The Community have taken steps ***.**

DDDD. Iran is a hard intelligence target, comparable to Russia and China. The regime appears to be highly sensitised to the threat of foreign intelligence work against it (the Committee noted in particular the regime's domestic monitoring system, *). The Intelligence Community's access to Iran is ***.**

EEEE. While SIS continues to *, the tight control the regime exercises ***.**

FFFF. Overall, the Intelligence Community have * coverage of Iran's capability, *** understanding of its intent, particularly in relation to Iran's ***. Given the potential for misunderstanding and miscalculation between Iran and Israel, this is of the utmost concern.**

GGGG. We welcome the new National Security Act 2023, which will fill important legislative gaps in tackling state threats. However, other gaps will remain unless the Official Secrets Act 1989 is reformed. The Government now appears to be backtracking on its commitment to Parliament to take this forward: this is of significant concern given the problems with the current regime.

HHHH. No decision has yet been taken as to whether Iran would be designated under the Enhanced Tier of the Foreign Influence Registration Scheme. While there are processes to be followed, we would nevertheless be surprised if Iran were not deemed worthy of inclusion under the Enhanced Tier – if it were not, it is hard to see which countries would be.

IIII. The UK has imposed financial sanctions on 508 individuals and 1,189 entities relating to Iran. The majority of these are companies involved with the nuclear programme, but they also include sanctions for human rights issues.

JJJJ. Given the scepticism we heard from External Experts as to the efficacy of sanctions, the Government should reconsider whether sanctions will in practice deliver behavioural change, or in fact unhelpfully push Iran towards China.

KKKK. We recognise the complexities inherent in a decision of whether or not to proscribe the Islamic Revolutionary Guard Corps. It is clear that such a decision would come with diplomatic implications: it appears that the real problem is that the Government is paralysed by the legal and practical difficulties around proscription of a state organisation – given that membership of an organisation proscribed in the UK carries a custodial sentence, which would apply to around a quarter of the Iranian Cabinet. The Government should fully examine whether it would be practicable to proscribe the Islamic Revolutionary Guard Corps and, if so, detail the competing arguments in a full statement to Parliament.

LLLL. The primary mechanism by which the Government responds to the Iranian physical threat is * a police-led process. We note the significant increase in the number of cases considered relating to Iran, and the successes of the operation in providing advice and protection.**

MMMM. The Committee was provided with numerous examples illustrating the increasing intent by the Iranian Intelligence Services to conduct lethal operations in the UK: we commend the efforts of MI5 and the police in response to what is now a serious threat.

NNNN. Given that Iran does not view attacks on dissident, Jewish and Israeli targets in the UK as constituting attacks on the UK, we encourage the Government and its international partners to make it clear to Iran – at every opportunity – that such attacks would indeed constitute an attack on the UK and would receive the appropriate response.

OOOO. The use of tools such as protective briefings and disruptive immigration measures has been successful in demonstrating to Iran that the UK is a hard operating environment. However, that has not stopped it from seeking to operate agent networks here.

PPPP. The Iranian espionage threat manifests itself acutely in the cyber domain, since cyber espionage represents an easier way for Iran to gain information which it would not necessarily be able to obtain within the UK due to the difficult operating environment.

QQQQ. It is essential to 'raise the resilience bar': if there is good cyber security and resilience across the UK, then it is less likely that Iran's * cyber-attacks will be successful. The National Cyber Security Centre's work to illuminate the tools and techniques used by Iranian cyber groups, and to warn UK organisations that they are being targeted, is therefore key to defending the UK.**

RRRR. The Committee has previously expressed concerns about Government complacency in allowing Russian pre-positioning for an attack through widespread penetration of UK Critical National Infrastructure. It is vital that the same mistakes are not made in relation to Iran – particularly given Iran's proven capability to cause serious disruption to essential services.

SSSS. The UK must raise the cost to Iran of it launching a cyber-attack on the UK, so as to deter it from doing so: public attribution of attacks is a valuable tool (albeit not without risk).

TTTT. The National Cyber Force was established in 2020 with specific responsibility for offensive cyber activity. Such operations have *. The Committee recognises the time and resource required in mounting such operations.**

UUUU. The Committee was surprised to hear that the Intelligence Community had successfully concluded * counter-cyber operations against Iran (i.e. operations to disrupt Iranian cyber-attacks) in the 12 months ***.**

VVVV. There are a number of boards, taskforces, working groups and reviews all working on the Government response to state interference. We question whether all are required: inevitably there will be duplication of time, effort and money. The Committee notes the tendency for there to be too many bodies co-ordinating at the expense of those bodies doing the actual front-line work.

WWWW. The Committee has yet to see the outcomes which the Defending Democracy Taskforce has been established to achieve, nor any indication that it has the authority to drive these outcomes forward across Government. It is unclear whether it truly represents a step forward in the Government's approach or simply yet another co-ordinating structure. We recommend that the Taskforce should set out its objectives and achievements in an annual statement to Parliament.

XXXX. Work to tackle disinformation and work to protect the security of the UK's democratic processes is clearly linked. The Committee considers that Parliament should be provided with a clear statement as to the work that will be completed ahead of the next General Election, with the associated classified material being provided to this Committee.

YYYY. The Committee recommends that the Government strengthen guidance to Parliament on vetting of staff employed in MPs' offices, in the context of recent high-profile allegations of espionage carried out by Parliamentary staffers.

ZZZZ. Whilst we are reassured that the Home Office is now investigating the threat posed by Iranian-aligned cultural groups – particularly the Islamic Centre of England – it is important that the Home Office's research is followed up with specific and timely action to ensure any threat from radicalisation, promotion of extremist material, and intimidation of UK-based students and diaspora is addressed.

AAAAA. We recognise that the Iranian nuclear programme, though one of the most difficult elements of work on Iran, is also the most important.

BBBBB. The Community have * in their understanding of *** weaponisation and *** the initial stages of weapons development. The UK – and perhaps the rest of the international community – may therefore have *** notice period before Iran is able to conduct a nuclear weapons test. *** is a priority across the entire Intelligence Community.**

CCCCC. GCHQ and SIS reporting has provided crucial insights into *, directly informing the tactics and policies pursued by HMG: their continuing insight is essential as the UK seeks to discourage Iranian nuclear escalation.**

DDDDD. The Intelligence Community seeks * Iran's nuclear programme ***. While we appreciate that such activity is difficult, and must be carefully considered, we found this surprising because of the *** priority given to Iran's nuclear programme in the National Security Council Iran Strategy.**

EEEEE. Given the volatility of the situation, the potential for misunderstanding and miscalculation by Iran, and the possibility for rapid escalation, it is not unrealistic to think that at some point it could become necessary to evacuate UK nationals in the region. The Committee notes the importance of proper preparation for a possible evacuation. * the Government must ensure that it has learnt the lessons from recent evacuation operations such as the withdrawal from Afghanistan.**

FFFFF. We note that work to * and are reassured that ***.**

GGGGG. The Government should use all the tools at its disposal to degrade the relationship between Iran and groups such as Al-Qaeda and Lebanese Hizbollah, including publicly calling out Iran's attempts to protect such terrorist groups.

ANNEX B: CODE WORDS

725. In some instances in this Report, we have substituted an ISC-specific code word where it has been necessary to refer to the name of an operation or project, in order to protect classified information. No significance is intended by, nor should be inferred from, the matching of code words to real operation names. The ISC code words have no operational significance.

ANISE	***
CARAWAY	***
CARDAMOM	***
GINGER	***
JUNIPER	***
KOKUM	***
MACE	***
NUTMEG	***
PAPRIKA	***
PEPPER	***
SAFFRON	***
SESAME	***
TAMARIND	***
TURMERIC	***

In one instance in this Report, we have substituted a publicly used name or designator for its classified equivalent.

CHARMING KITTEN	***

ANNEX C: LIST OF WITNESSES

Ministers

The Rt Hon. James Cleverly MP – Foreign Secretary

The Rt Hon. Suella Braverman KC MP – Home Secretary

Officials

CABINET OFFICE

Sir Simon Gass KCMG CVO – Chair, Joint Intelligence Committee

Matthew Collins CBE – Deputy National Security Adviser, National Security Secretariat

Other officials

FOREIGN, COMMONWEALTH AND DEVELOPMENT OFFICE (FCDO)

Vijay Rangarajan CMG – Director General, Afghanistan, Pakistan, Overseas Territories, Middle East and North Africa

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Officials

HOME OFFICE

Chloe Squires – Director General, Homeland Security Group

Other officials

MINISTRY OF DEFENCE

Adrian Bird CB – Chief of Defence Intelligence

Other officials

SECRET INTELLIGENCE SERVICE (SIS)

Sir Richard Moore KCMG – Chief

Other officials

SECURITY SERVICE (MI5)

Sir Ken McCallum KCB – Director General

Other officials

External Expert witnesses

Professor Ali Ansari, Professor of Iranian History, University of St Andrews

The Rt Hon. the Baroness Ashton of Upholland LG GCMG, High Representative of the European Union for Foreign Affairs and Security Policy (2009–2014)

Ambassador John Bolton, United States National Security Adviser (2018–2019)

Sir Richard Dalton KCMG, UK Ambassador to Iran (2002–2006)

Professor Anoush Ehteshami, Professor of International Relations, Durham University

Dr Sanam Vakil, Director, Middle East and North Africa Programme, Chatham House

ISBN 978-1-5286-5785-3
E03390063