The IRGC’s Cyber Threat to the United Kingdom: A Strategic Briefing

By Catherine Perez-Shakdam - Executive Director Forum for Foreign Relations

Foreword

By all rights, we ought to be done with empire. With empires of territory, of ideology, of belief systems that parade as divine destiny and yet run on fear, repression, and the barrel of a gun — or, as it increasingly happens, the whisper of a keystroke. And yet, here we are.

The document you hold in your hands does not concern itself with fantasies. It speaks, in measured but urgent tones, of a very real menace — not some sinister Bond villain, but an entrenched, well-funded and ideologically turbocharged arm of the Iranian state: the **Islamic Revolutionary Guard Corps (IRGC)**. The IRGC are more than a mere conventional army. The IRGC's legal mandate, enshrined in Iran's 1979 constitution, is that of an *"ideological army"* charged with *"extending the sovereignty of God's law throughout the world."* To fulfil this mission, the IRGC are also highly skilled, well-funded, and have developed strong capabilities in expertise in electronic- and psychological warfare. The IRGC infiltrates minds as easily as servers; their weapons include malware, misinformation, and martyrdom.

What makes the matter so pressing — and so directly relevant to the citizens and Parliamentarians of the United Kingdom — is that the IRGC's theatre of cyber mischief is not some distant sandbox in the Middle East, but our own universities, our institutions, Parliament, and even our multicultural, multi-confessional neighbourhoods. The IRGC has found ways to use our openness as a cudgel against us. Our tolerance, our liberty — the very things that make Britain proud — become the soft underbelly through which the IRGC administer their poison and through which they seek to advance the cause of the Islamic Revolution.

This report charts the scope of the IRGC's threat to the United Kingdom, as well as the specifics of the IRGC's method and madness. It makes clear that the IRGC is a systemic risk to our national security and to the integrity of our civic life. This report is respectful to British Muslims and to Muslims across theMiddle East, as these are the very first communities to suffer when tyrants come knocking with scripts of radicalism and delusions of empire wrapped in the language of Islamic belief .

This report aims to provoke a measure of alarm in UK Parliamentarians that is proportionate, responsible and urgent compared to the imminent and immediate threats to the UK from the IRGC. Alarm is the necessary, responsible, and sober response to these threatsUK Parliamentarians must, now, clearly articulate that urgent action must be taken to eliminate the threats posed by the IRGC and to protect our core freedoms.

So read on. Carefully. Critically. Courageously.
For the guardianship of a free society begins with understanding what threatens it — and calling that threat by its name.

By Catherine Perez-Shakdam - Executive Director Forum for Foreign Relations

Introduction

The Islamic Revolutionary Guard Corps (IRGC)—once known chiefly for orchestrating foreign insurgencies and exporting theocratic revolution—has rapidly evolved into one of the world's most dangerous cyber actors. Today, it wages a hybrid war that fuses digital sabotage with ideological subversion, and the United Kingdom has become one of its prime targets.[1]

No longer limited to shadowy operations in Lebanon, Syria or Iraq, the IRGC now extends its reach deep into the digital arteries of the UK. British officials, academic institutions, journalists, dissidents, and entire communities have been subject to a concerted and increasingly aggressive campaign of espionage, hacking, intimidation, and psychological warfare. Its foot soldiers are not only IRGC cyber units in Tehran, but a web of proxies—hacker collectives, "activist" NGOs, fake media outlets, and social media avatars—all designed to erode Britain's defences from within.

In 2022, the head of MI5 publicly disclosed that Iran had orchestrated at least ten abduction or assassination plots in the UK within a single year, describing Iran's activities as "the most sustained hostile threat" from any state besides Russia. Much of this threat stems from the IRGC, which controls Iran's intelligence apparatus and deploys both online and offline operatives. That same year, IRGC-linked hackers breached British parliamentary emails, targeted MPs critical of the regime, and penetrated university systems conducting research on Iran's influence operations.[2]

But digital intrusion is only half the story. The IRGC also exports disinformation and extremism—particularly to Britain's Arab and Muslim communities—through online indoctrination campaigns aimed at spreading Tehran's revolutionary ethos. These are not isolated incidents but part of a strategic effort to radicalise, polarise, and ultimately mobilise British audiences in service of Iran's geopolitical objectives.

This briefing sets out to expose the full extent of this threat. It will:

- dissect the IRGC's evolving cyber warfare strategy and capabilities;

---

[1] United Kingdom Parliament, House of Commons Foreign Affairs Committee, *No Protection, No Freedom: The Foreign Policy Implications of the IRGC's Hostile Activities*, HC 313 (2023), 9–11, https://committees.parliament.uk/publications/40891/documents/199902/default/.

[2] MI5 Director General Ken McCallum, speech at Thames House, London, November 16, 2022, quoted in Patrick Wintour, "Iran Plotted to Kidnap or Kill UK-Based People 10 Times Last Year, Says MI5," *The Guardian*, November 16, 2022, https://www.theguardian.com/uk-news/2022/nov/16/iran-kidnap-kill-uk-people-mi5.

- document specific cases of cyber aggression against British institutions and individuals;
- analyse the use of proxies and ideological front groups as force multipliers;
- assess the impact on vulnerable communities within the UK, especially Arabs and Muslims;
- and provide strategic policy recommendations, foremost among them the urgent need to proscribe the IRGC as a terrorist organisation under UK law.

The threat is no longer hypothetical. It is present, persistent and urgent. Unless addressed with clarity, coherence and resolve, the IRGC threat will only deepen. This is not merely a matter of cybersecurity. It is a matter of national security, community resilience, and the preservation of democratic sovereignty.

The IRGC: a force that is malign, malevolent,and current threatening British interests at home and those of our allies

The IRGC's agenda is driven by the Islamic Republic's core strategic goals. Foremost among these is regime survival – ensuring the stability and longevity of Iran's ruling system. The IRGC has developed a mastery of the tools of cyber- and psychological-warfare to neutralise dissent at home and abroad. Other objectives include *"preserving Iran's Islamic values"* by combating cultural influence, defending Iran's territory and population, promoting economic growth (for which stolen intellectual property is a boon), and exporting Iran's revolutionary ideology and influence across the region. The IRGC's very mandate, enshrined in Iran's 1979 constitution, is that of an *"ideological army"* charged with *"extending the sovereignty of God's law throughout the world."* In cyberspace, this translates to spreading the Islamic Republic's worldview and empowering pro-Iran movements abroad, and neutralising dissent or threats that arise within Iran.[3]

A deep-seated sense of historical grievance and conventional military inferiority drives Iran to *"offset the advantages of its more powerful adversaries"* through asymmetric tactics like cyber warfare. In short, the IRGC's growing cyber arsenal is now a central pillar of Iran's strategy to project power beyond its borders while protecting the regime at home.[4] This has serious implications for the UK, which is very much in the top tier of perceived adversaries (after the United States and Israel).

---

[3] Islamic Republic of Iran, *Constitution of the Islamic Republic of Iran*, 1979, Article 150, https://www.refworld.org/docid/3ae6b56710.html.

[4] U.S. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 2022, 20–21, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

IRGC Cyber Warfare Capabilities and Strategic Goals

The IRGC has rapidly transformed itself into the dominant player in Iran's offensive cyber program. By the mid-2010s, it had recruited *"thousands of personnel"* and built a dedicated Electronic Warfare and Cyber Defense Organization to conduct attacks in cyberspace.[5] Today, the IRGC sits atop a sprawling cyber apparatus that includes not only its in-house specialists but also an array of semi-independent hackers, contractors, and "hacktivist" collectives operating under its patronage. In effect, the IRGC has weaponised Iran's tech sector and youthful talent pool: roughly 18% of Iranian university students study computer science, and many tech graduates are funneled via compulsory service into the IRGC or intelligence ministry.[6] This investment has paid dividends. Western assessments now rank Iran among the world's most active cyber powers – arguably at the *"top of the second tier"* of cyber-capable states – with a demonstrated willingness to carry out aggressive and even destructive operations. By 2016 Iran was reportedly spending over $1 billion annually on its cyber capabilities, a budget on par with some leading cyber powers (the UK spent an estimated $2 billion that year). Tehran's cyber budget increased twelvefold between 2013 and 2021, underscoring how strategically critical this domain has become to Iran's regime.[7]

Strategic drivers

Several critical factors drove the IRGC's rapid investment in cyber capabilities over the past decade. Internally, the Iranian regime was deeply shaken by the 2009 Green Movement protests, when millions of Iranians took to the streets to contest alleged electoral fraud. Protesters used social media platforms — particularly Twitter, Facebook, and SMS messaging — to organise demonstrations and bypass state-controlled media. For the first time, the Iranian leadership faced a mass mobilisation catalysed and coordinated through digital tools. The experience underscored the disruptive potential of cyberspace not just for foreign propaganda, but for internal dissent. In the aftermath, the regime — and especially the IRGC — concluded that cyber operations would be essential not only for surveillance and repression, but also for shaping narratives and maintaining control over information flow within Iran.

---

[5] Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*, Carnegie Endowment for International Peace, January 2018, 6–7, https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134.

[6] John Hultquist, "Iranian Cyber Capabilities: Espionage, Sabotage, and Influence," testimony before the U.S. House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, April 26, 2018, https://www.congress.gov/115/meeting/house/108205/witnesses/HHRG-115-HM08-Wstate-HultquistJ-20180426.pdf.

[7] James A. Lewis, *The Hidden Costs of Cybercrime*, Center for Strategic and International Studies (CSIS), December 2020, https://www.csis.org/analysis/hidden-costs-cybercrime.

Externally, the turning point came in 2010 with the discovery of Stuxnet, a sophisticated cyber weapon allegedly developed by the United States and Israel. The malware successfully targeted and sabotaged Iran's uranium enrichment centrifuges at Natanz, setting back the country's nuclear programme without a single shot being fired. The attack was both humiliating and illuminating for Tehran: it revealed how vulnerable Iran's critical infrastructure was to foreign cyber intrusion, and how warfare had expanded into a new, invisible domain.

Together, these two events — the internal unrest of 2009 and the foreign sabotage of 2010 — crystallised a doctrine of cyber urgency within the IRGC. Facing adversaries with vastly superior conventional forces and high-tech arsenals, Iran embraced cyber power as an asymmetric equaliser. The IRGC's cyber strategy has since been shaped by this deep-seated sense of insecurity, prompting Tehran to invest heavily in building offensive and defensive capabilities designed to deter, retaliate, and project power through non-kinetic means.

Iran's leadership sees cyberspace as an ideal arena for "asymmetric" warfare – a means to hit back at stronger foes (the US, Israel, and their allies) without conventional military confrontation. As analysts note, Tehran's doctrine of *"forward defense"* includes taking the fight beyond its borders via cyber operations that deter enemies and exact costs for sanctions or strikes. The IRGC's playbook emphasises ambiguity and deniability: cyber attacks can be hard to attribute, allowing Iran to push boundaries while avoiding full-scale retaliation.[8] Indeed, the IRGC often hides its hand by using front companies, criminal contractors, and patriotic "hacktivists" as proxies. Iranian malware is abandoned once exposed, and the membership of hacker groups is kept fluid. *"The IRGC reportedly employs trusted intermediaries to outsource [cyber] contracts…at times employing several contractors for a single operation,"* a 2024 study observed.[9] These cut-outs provide plausible deniability even as they ultimately answer to IRGC direction. Iranian cyber units also collaborate with foreign partners – notably Russia and to a lesser extent China – to bolster their capabilities, learning new tactics and leveraging advanced tools like artificial intelligence.[10]

Offensive capabilities

Over the past decade, the IRGC has developed a full spectrum of offensive cyber tools to advance Iran's national objectives. As one expert assessment succinctly states, *"Iran has developed offensive cyber capabilities for purposes of disruption and destruction,*

---

[8] Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*, Carnegie Endowment for International Peace, January 2018, 4–6, https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134.

[9] Institute for Strategic Dialogue (ISD), *Networks of Influence: Mapping Iran's Cyber Operations and Proxy Architecture*, March 2024, 17, https://www.isdglobal.org/research/publications/networks-of-influence-irgc-cyber-2024/.

[10] Institute for Strategic Dialogue (ISD), *Networks of Influence: Mapping Iran's Cyber Operations and Proxy Architecture*, March 2024, 17, https://www.isdglobal.org/research/publications/networks-of-influence-irgc-cyber-2024/.

espionage, and information operations.". In practice, this means IRGC-linked actors have shown the ability to:

Sabotage critical infrastructure

IRGC forces have built and deployed an arsenal of sophisticated malware, specifically designed to penetrate the computer systems that power essential public utilities. Once inside the target system, the IRGC is able to disable key functions, delete vital data, or deface the screens and user interfaces. Irangave the world a taste of this in 2012 when an IRGC-affiliated virus (*Shamoon*) wiped tens of thousands of Saudi Aramco computers.[11] More recently, in late 2023,[12] IRGC cyber operatives known as "CyberAv3ngers" targeted industrial programmable logic controllers (PLCs) used in water treatment facilities, defacing systems with messages "Down with Israel". Victims spanned multiple countries including the UK, where the National Cyber Security Centre (NCSC) observed Iranian attempts to compromise PLC devices in British critical infrastructure as part of this campaign. Such attacks demonstrate Iran's capability – and intent – to inflict disruptive or destructive effects via cyber means.

Steal sensitive data and conduct espionage

The IRGC's electronic espionage capabilities present a serious threat to Western powers through both their effectiveness and scalability. The IRGC directs multiple Advanced Persistent Threat (APT) groups focused on espionage, gathering sensitive military and industrial information, and collecting material for potential blackmail of Western political and business leaders.

Key IRGC-operated APT groups include menagerie of so-called "Kitten teams" operating under aliases such *"Domestic Kitten"* (which focuses on surveilling Iranian dissidents at home and abroad, including in the UK), *"Charming Kitten"* (which conducts phishing and social media espionage against foreign targets), and *"Magic Kitten"* (which spies on domestic regime opponents). Other units specialise in credential theft and email intrusions, often by impersonating journalists or conference organizers to circumvent standard security measures.

Their targets include government officials, defense contractors, academics, dissidents, and businesses worldwide. The stolen information advances Iran's strategic objectives by providing military intelligence, industrial intellectual property, and personal data on regime critics. By 2019, U.S. intelligence assessed that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."

The scale of these operations is significant. The IRGC-contracted Mabna Institute breached over 300 universities across 22 countries, including the UK, to acquire

---

[11] Chris Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (April–May 2013): 81–96, https://doi.org/10.1080/00396338.2013.784468.

[12] Dragos Inc., *Iranian Cyber Operations: CyberAv3ngers Target ICS and PLCs*, Threat Intelligence Brief, November 2023, https://www.dragos.com/blog/industry-news/iran-cyberavengers-target-ics/.

research data. Iranian cyber units have also accessed email accounts of prominent figures, demonstrated by their 2017 breach of UK MPs' personal correspondence, gathering intelligence and potentially acquiring material to embarrass those deemed hostile to Iran (more detail on both Iranian cyber-campaigns is included later in this report).

.[13]Run influence and disinformation campaigns

The IRGC's cyber mission is not only about hacking but also propaganda and ideological warfare. Like Russia, Iran has created networks of fake online personas, "troll farms," and propaganda websites to shape narratives globally. Facebook and Twitter have repeatedly dismantled Iranian disinformation networks. For instance, in 2020 Facebook removed a sprawling set of over 500 accounts tied to Iran's state broadcaster (IRIB) that targeted users in the UK, US and beyond. Posing as independent media or charities, these accounts pushed narratives aligned with Tehran's agenda – even inserting themselves into UK domestic debates by amplifying support for Scotland's 2014 independence referendum. The IRGC, often via the Basij paramilitary (an Iran-wide network of volunteers), also operates a *"cyber propaganda machine"* to disseminate regime messaging and Shiite Islamist dogma at home and abroad. This includes multilingual "news" sites that mask their Iranian origin, orchestrated social media hashtags, and fabricated videos (in some cases using AI-generated deepfakes to lend false credibility). These disinformation operations serve to bolster Iran's image, recruit sympathisers, and sow discord among its adversaries' societies.

These capabilities are wielded in a "flexible, layered" hybrid warfare strategy that integrates cyber tools with Iran's conventional and clandestine operations. The IRGC coordinates closely with other elements of Iran's security apparatus in cyberspace, blurring lines between military, intelligence, and paramilitary actors. The IRGC's own cyber command takes primary charge of offensive campaigns, but it leverages the Basij militia to provide manpower and cover. The Basij has formed some 1,000 "cyber battalions" across Iran and outsources tasks to ~50 patriotic hacker groups.[14] These range from well-known outfits like the "Iranian Cyber Army" and "Ashiyane Digital Security" to the aforementioned menagerie of codenamed "Kitten" teams. By operating through such cut-outs, the IRGC conceals its hand while tapping into a pool of semi-deniable cyber talent.

Iranian cyber cells also collaborate, share tactics with, and learn from allied state actors – there are documented instances of Tehran aligning with Moscow on technology initiatives to reduce reliance on Western software, and Iran's hackers have shown a penchant for *"learning cyber capabilities from Moscow"* and even adopting Russian-style tactics. All these factors make the IRGC's cyber enterprise highly agile

---

[13] U.S. Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, January 29, 2019, 5–6, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[14] Behnam Ben Taleblu, *Tehran's Cyber Army: How Iran Builds and Uses Its Online Arsenal*, Foundation for Defense of Democracies, October 2020, 3–5, https://www.fdd.org/analysis/2020/10/15/tehrans-cyber-army/.

and unpredictable. It can strike targets ranging from critical infrastructure to Twitter feeds, using methods that evolve quickly to bypass defenses.

Documented IRGC Cyber Attacks Targeting UK Interests

Iran's hostile cyber activities are not abstract threats – they have already struck high-value targets in the United Kingdom, often via IRGC-linked proxies and cut-outs. A review of documented incidents reveals a pattern of intrusions and influence operations reaching into British academia, government, civil society, and even personal accounts. These cases illustrate the breadth of the IRGC's campaign against the UK, and expose the methods – from hacking collectives to media fronts – that Tehran employs to achieve its aims.

The Parliament Email Breach (2017)

In June 2017, a cyberattack hit the email system used by MPs and peers at Westminster, compromising dozens of parliamentary accounts (including that of then-Prime Minister Theresa May).[15] Initial suspicion fell on Russia or North Korea, but an intelligence assessment later attributed the attack to Iran. This appears to have been the *first significant Iranian cyber-attack on a British target*, catching observers off guard. The hackers used a brute-force attack to exploit weak passwords and break into inboxes. While Iran never officially claimed responsibility, British officials privately concluded the IRGC or its affiliates were behind the breach. The motive may have been espionage – harvesting sensitive communications – or even potential blackmail material, as compromised emails could expose personal or political secrets This intrusion into the heart of UK democracy signaled that Iranian cyber units were willing to target the most high-profile British institutions. The attack also underscored a lax cybersecurity culture (many accounts were protected by weak passwords) that Iran was quick to exploit. Though the immediate damage was contained by prompt IT response (password resets and network blocks), the incident was a wake-up call that IRGC cyber spies were actively probing UK government networks.[16]

---

[15] Paul Croft and Gordon Rayner, "Cyber Attack on Westminster: Hackers Target MPs in Attempt to Access Parliament Accounts," *The Telegraph*, June 24, 2017, https://www.telegraph.co.uk/news/2017/06/24/cyber-attack-westminster-hackers-target-mps-attempt-access/.

[16] Kim Sengupta, "Iran Behind Cyber-Attack on UK Parliament, Security Officials Believe," *The Independent*, October 14, 2017, https://www.independent.co.uk/news/uk/politics/iran-cyber-attack-uk-parliament-theresa-may-mps-hackers-a8001266.html.

University Espionage – The Mabna Institute Hacks (2013–2018)

Beginning in 2013, Iran's Mabna Institute spearheaded one of the most expansive academic cyber-espionage campaigns ever exposed. Operating as a front organisation for the Islamic Revolutionary Guard Corps (IRGC), Mabna conducted highly coordinated attacks on universities and academic institutions across the globe. Its objective was not sabotage, but intellectual plunder: the systematic theft of research, credentials, and proprietary data to fuel Iran's strategic advancement in science and technology.

Over the course of five years, Mabna's operatives breached the systems of at least 144 universities in the United States and 176 more in 21 other countries, including leading institutions in the United Kingdom. Using deceptive phishing emails and spoofed identities — often impersonating faculty, librarians, or research staff — the hackers gained access to university library portals and research databases. From there, they exfiltrated over 30 terabytes of academic content, including journal articles, doctoral theses, and sensitive scientific data in fields ranging from engineering and chemistry to international relations and defence studies.

The campaign was sophisticated and tailored. Rather than indiscriminate hacking, Mabna's activities reflected clear intelligence priorities, targeting research likely to be of military, industrial, or ideological value to the regime. The stolen data was either channelled to Iranian state institutions — particularly the IRGC — or resold on black-market platforms inside Iran, circumventing international sanctions that limited Iran's access to high-quality academic resources and technology.

In March 2018, the United States Department of the Treasury formally sanctioned the Mabna Institute, accusing it of acting "on behalf of the IRGC" and labelling its operations as part of Iran's broader state-directed cyber strategy. The U.S. Justice Department simultaneously indicted nine Iranian nationals associated with Mabna for stealing intellectual property worth an estimated $3.4 billion.

British authorities also responded. The UK's National Cyber Security Centre (NCSC) publicly condemned the activity, stating with "high confidence" that Mabna was "almost certainly responsible" for the campaign affecting UK universities. The NCSC warned that the targeting of Britain's higher education sector was not just a matter of data theft, but a strategic threat to national innovation and competitive advantage.

From a broader perspective, the Mabna case exemplifies the IRGC's preference for deniable, outsourced cyber operations. By using a nominally private institute to execute state-sanctioned cyber theft, Iran masked its involvement while reaping the strategic benefits. The campaign also highlights a central pillar of Iran's cyber doctrine: leveraging cyber tools to leapfrog economic and technological constraints imposed by sanctions and diplomatic isolation.

In practical terms, Mabna enabled Tehran to accelerate its domestic R&D without the burden of original innovation, effectively copying rather than creating. This not only supported Iran's ambitions in areas like nuclear development and military technology

but also served the ideological imperative of resistance: defying the West while simultaneously exploiting its openness and infrastructure.

Beginning in 2013, Iran's Mabna Institute spearheaded one of the most expansive academic cyber-espionage campaigns ever exposed. Operating as a front organisation for the Islamic Revolutionary Guard Corps (IRGC), Mabna conducted highly coordinated attacks on universities and academic institutions across the globe. Its objective was not sabotage, but intellectual plunder: the systematic theft of research, credentials, and proprietary data to fuel Iran's strategic advancement in science and technology.[17]

Over the course of five years, Mabna's operatives breached the systems of at least 144 universities in the United States and 176 more in 21 other countries, including leading institutions in the United Kingdom. Using deceptive phishing emails and spoofed identities — often impersonating faculty, librarians, or research staff — the hackers gained access to university library portals and research databases. From there, they exfiltrated over 30 terabytes of academic content, including journal articles, doctoral theses, and sensitive scientific data in fields ranging from engineering and chemistry to international relations and defence studies.

The campaign was sophisticated and tailored. Rather than indiscriminate hacking, Mabna's activities reflected clear intelligence priorities, targeting research likely to be of military, industrial, or ideological value to the regime. The stolen data was either channelled to Iranian state institutions — particularly the IRGC — or resold on black-market platforms inside Iran, circumventing international sanctions that limited Iran's access to high-quality academic resources and technology.

In March 2018, the United States Department of the Treasury formally sanctioned the Mabna Institute, accusing it of acting "on behalf of the IRGC" and labelling its operations as part of Iran's broader state-directed cyber strategy. The U.S. Justice Department simultaneously indicted nine Iranian nationals associated with Mabna for stealing intellectual property worth an estimated $3.4 billion.

British authorities also responded. The UK's National Cyber Security Centre (NCSC) publicly condemned the activity, stating with "high confidence" that Mabna was "almost certainly responsible" for the campaign affecting UK universities. The NCSC warned that the targeting of Britain's higher education sector was not just a matter of data theft, but a strategic threat to national innovation and competitive advantage.

From a broader perspective, the Mabna case exemplifies the IRGC's preference for deniable, outsourced cyber operations. By using a nominally private institute to execute state-sanctioned cyber theft, Iran masked its involvement while reaping the strategic benefits. The campaign also highlights a central pillar of Iran's cyber doctrine:

---

[17] U.S. Department of Justice, "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

leveraging cyber tools to leapfrog economic and technological constraints imposed by sanctions and diplomatic isolation.

In practical terms, Mabna enabled Tehran to accelerate its domestic R&D without the burden of original innovation, effectively copying rather than creating. This not only supported Iran's ambitions in areas like nuclear development and military technology but also served the ideological imperative of resistance: defying the West while simultaneously exploiting its openness and infrastructure.

In sum, the Mabna Institute's global academic hacking campaign illustrates the scale, precision, and audacity of the IRGC's cyber strategy — a campaign conducted not with bombs or bullets, but with keystrokes, false credentials, and stolen research. It remains a cautionary tale for open societies: that even their most noble institutions, such as centres of learning, can become targets in the new arena of hybrid warfare.

The Mabna case is a textbook example of the IRGC's *espionage-through-proxy* approach: instead of uniformed IRGC officers hacking UK universities, it hired criminal hackers under a nominally private institute to do the job, maintaining deniability. But the strategic payoff – enriching Iran's knowledge base and military R&D – aligned perfectly with IRGC and regime interests. UK Foreign Office Minister Lord (Tariq) Ahmad noted that by "stealing intellectual property from [our] universities, these hackers attempted to gain technological advantage at our expense," calling it a direct assault on UK prosperity and innovation.[18]

Targeting of British Individuals – Phishing and Personal Account Compromises

Beyond headline-grabbing breaches, Iranian state-linked hackers have engaged in persistent phishing and account hijacking campaigns against British citizens – especially those in policy, media, and defense circles. In January 2023, the NCSC issued an unusual public alert warning that IRGC-associated groups were *"ruthlessly"* targeting UK politicians, journalists, researchers, and activists with sophisticated phishing ploys. Elements within Iran's cyber apparatus impersonated conference organisers or journalists to trick targets into clicking malicious links. Using these social engineering methods (sometimes over a series of interactions to build trust), the hackers were able to steal login credentials and access private communications. The goal was espionage or influence rather than financial gain: stolen emails could yield intelligence or be leaked strategically.

[18] U.S. Department of Justice, "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

NCSC officials have commented that these campaigns had intensified in the UK, likely spurred by geopolitical tensions (Iran seeking leverage amid crises like the Ukraine war and nuclear talks). The specifics of each incident typically remain classified, but the public warnings and occasional press reports make clear that IRGC cyber units view Britain's political and analytic communities as high-value targets – and the UK as a fertile ground for espionage and disinformation. The UK is not alone in this: Iranian phishing operations have similarly struck officials in the US and EU. However, the focus on UK groups is notable; one security memo cited by the Guardian said Iranian hackers had *"stepped up their activities in the UK… operating in the US and other NATO countries"* simultaneously. This reflects Iran's intent to penetrate Western decision-making circles and possibly pre-empt or retaliate against policies it dislikes (such as sanctions or criticism of Iran's human rights record).[19]

Propaganda "Media Fronts" and Influence Operations in the UK

IRGC cyber aggression also manifests as information warfareTheir tactics include using inauthentic accounts to join social media debates, creation of glossy propaganda videos for platforms like YouTube, coordination with sympathetic Western fringe outlets, and the continued operation of discredited pseudo-media channels such as PressTV to seed stories favourable to Iran. A revealing case came in May 2020,[20] when Facebook exposed and banned an IRIB-linked network that had covertly operated since at least 2011. This network ran hundreds of Facebook and Instagram accounts pushing pro-Iran and anti-West narratives to British users, as well as users in countries ranging from Algeria to Zimbabwe. IRGC-backed operators would masquerade as independent news outlets or charitable organisations, often posting on local conflicts with a pro-Tehran spin. In the UK's case, researchers found that Iranian accounts had already directly interfered in British politics – for example, in 2014 some fake personas that could be traced back to Iranian entities actively promoted Scottish separatism during the independence referendum, seemingly an apparent experiment with fomenting divisions in a Western country. Though those efforts were limited and largely ineffectual, they show Iran's willingness to copy Russian-style interference tactics.

More recently, Iranian influence accounts in English have focused on discrediting UK and US foreign policy (e.g. portraying Western sanctions as cruel, or spreading conspiracy theories that blame Britain and America for Middle East turmoil). The *"London office"* of Iran's English-language broadcaster Press TV. Despite Ofcom removing its UK broadcast license in 2012ked, Press TV continues to 'broadcast' its content via online video-distribution channels. Press TV's editorial strategy seems tailored to appeal specifically to British Muslim audiences, often amplifying narratives favorable to Iran (such as highlighting UK politicians critical of Saudi Arabia or Israel), and downplaying Iran's own misdeeds.

---

[19] Dan Sabbagh, "Iranian Hackers Target UK Think-Tank and Journalists in Espionage Campaign," *The Guardian*, May 15, 2022, https://www.theguardian.com/uk-news/2022/may/15/iranian-hackers-target-uk-thinktank-and-journalists-in-espionage-campaign.

[20] Facebook (Meta), *Removing Coordinated Inauthentic Behavior from Iran*, May 2020, https://about.fb.com/news/2020/05/removing-coordinated-inauthentic-behavior-from-iran/.

While harder to quantify than hacks, these information operations represent a concerted IRGC effort to sway public opinion and diaspora communities in the UK. The IRGC aims to undermine British public support for policies that counter Iran (e.g. opposition to the Iran nuclear deal or designation of Hezbollah as a terrorist group), and to advance Tehran's preferred ideological narratives on issues like Palestine, Islamophobia, and Middle East conflicts.

Other Notable Incidents

Iranian cyber actors have shown interest in UK infrastructure and private sector targets as well. In addition to the PLC sabotage attempt noted earlier, British cybersecurity firms have tracked Iranian intrusions into the networks of UK companies in the technology and telecommunications sectors (often as collateral in global campaigns). In 2021, for example, an Iranian group dubbed "TunnelVision" was detected exploiting Fortinet and Microsoft Exchange server vulnerabilities in European firms, including some in Britain, likely for espionage purposes.

The Iranian diaspora in Britain has also been subject to cyber intimidation.[21] Activists of Iranian heritage (journalists, human-rights defenders, opposition groups) report frequent phishing attempts and malware-laced messages seemingly from Iran's security services. In one high-profile case in late 2022, two British-Iranian journalists working in London (for Iran International TV) received credible warnings of an IRGC plot to assassinate them, forcing their media outlet to relocate overseas. The would-be assassins used cyber means to stalk the journalists online. And while th was ultimately a physical threat disrupted by UK authorities, it underlines how Iran's cyber operations and real-world terrorism often go hand-in-hand, directed by the IRGC.The IRGC's blended use of cyber tools alongside covert action is further exemplified by revelations that Iranian spies conducted surveillance of a UK-based Israeli embassy guard via social media before an alleged plot to attack the embassy – a plot foiled by MI5 in 2023.

Taken together, these examples paint a stark picture: the IRGC and its proxies have UK institutions and citizens in their crosshairs, using cyber means to penetrate, pilfer, propagandise, and even prepare the battlefield for potential violence. No sector is categorically off-limits – education, government, media, diaspora communities, and critical industries have all been impacted. This multi-faceted threat directly serves Iran's strategic objectives, as the next section explores.[22]

How IRGC Cyber Operations Serve Iran's Foreign Policy Agenda

[21] Mandiant Threat Intelligence, *UNC2448 Exploits Fortigate and Microsoft Exchange Vulnerabilities*, November 2021, https://www.mandiant.com/resources/blog/unc2448-espionage-iran.
[22] MI5 Security Service, Director General Ken McCallum, Annual Threat Update Speech, November 15, 2023, https://www.mi5.gov.uk/news/speech-by-mi5-director-general-ken-mccallum-2023.

Iran's cyber offensives against the UK do not occur in a vacuum – they are a means to an end, closely aligned with Tehran's geopolitical ambitions and ideological worldview. Each type of operation examined above (disruption, espionage/surveillance, and influence) advances specific Iranian foreign policy goals. Understanding these motivations is key to crafting effective countermeasures. In essence, the IRGC's cyber campaigns are a form of statecraft by other means: a tool of *"war by stealth"* that Iran wields to compensate for its conventional weakness, retaliate against adversaries, project power abroad, and export its revolution. Below we analyse how the IRGC's cyber activities serve Iran's agenda of disruption, surveillance, and influence – and by extension, how they threaten UK interests at a strategic level.

Disruption and Deterrence

Iran employs cyber attacks to disrupt the interests of countries it perceives as enemies – often as retaliation or warning shots – thereby serving a deterrent purpose. Lacking the military might to go toe-to-toe with Western powers, Tehran instead seeks to impose costs through deniable cyber strikes. This fits into Iran's broader doctrine of deterrence which includes proxy terrorism and missile threats; cyber is a newer but increasingly central pillar of that doctrine. For example, after Iran's nuclear program was struck by the Stuxnet virus (widely attributed to Israel and the US), Iranian hackers – likely under IRGC guidance – launched "Operation Ababil" in 2012, a wave of disruptive cyberattacks on U.S. banks that intermittently knocked banking websites offline. The message was clear: Iran could punch back in cyberspace for real-world pressure.

In the UK context, one can view the *2017 Parliament hack* in a similar light. It occurred at a tense moment in Iran-West relations (President Trump was threatening to scrap the Iran nuclear deal), and by breaching MPs' communications, Iran signaled it could penetrate the British political establishment's digital defences.[23] While no public "detonation" or destruction was carried out in that case, merely demonstrating access may have been meant to sow unease. Likewise, the targeting of industrial control systems in 2023 – specifically PLCs used in water facilities – had a geopolitical motive: Iranian hackers explicitly defaced systems with anti-Israel slogans as they sought out Israeli-made equipment to vandalise. In doing so, they caused collateral risk to UK infrastructure (since British utilities using that equipment were hit). Here Iran was pursuing its conflict with Israel via global cyber means, effectively using any connected system with Israeli components as a battlefield. The incident served Tehran's policy of confrontation with Israel and attempted to deter Israeli tech firms by showing they could become liabilities for foreign customers.

More broadly, every time Iran's cyber warriors successfully disrupt a Western asset – be it temporarily paralyzing a company's network or leaking embarrassing emails of a public figure – the regime scores a propaganda win and sends a deterrent signal. It

[23] Kim Sengupta, "Iran Behind Cyber-Attack on UK Parliament, Security Officials Believe," *The Independent*, October 14, 2017, https://www.independent.co.uk/news/uk/politics/iran-cyber-attack-uk-parliament-theresa-may-mps-hackers-a8001266.html.

showcases Iran's *"technological prowess and strategic capability in cyberspace"* aiming to make adversaries think twice before striking Iran. The IRGC's use of proxies amplifies this effect: when a fringe "hacktivist" group defaces a UK website or a mysterious outage hits a British company, Iran can deny involvement while quietly savouring the result. Notably, Tehran tends to calibrate its disruptive attacks to avoid all-out war, focusing on *"low-hanging fruit"* targets and symbolic blows. This aligns with FFR assessment that Iran remains a second-tier cyber power – less technically sophisticated than China or Russia – but one that compensates with boldness and strategic timing.

In sum, disruption via cyber allows the IRGC to project power disproportionate to Iran's size, serving foreign policy by retaliating for sanctions or strikes (e.g. the banking hacks in response to sanctions), attempting to deter future actions (e.g. warning the UK not to host anti-regime media), and generally raising the cost of opposing Iran. For the UK, this means that as long as London stands in opposition to key Iranian objectives (from Iran's nuclear expansion to its regional hegemony), it will continue to be a potential target for IRGC cyber disruption, chosen at a time and place that suits Tehran's narrative.

Espionage and Surveillance within British communities

Iran's Ministry of Intelligence and the IRGC's intelligence arm have long spied on Iranian exiles here and abroad through human means; now, cyber gives them unprecedented reach. The earlier reference to *"Domestic Kitten"* malware targeting dissidents in the UK and US highlights that the IRGC uses cyber tools to keep tabs on opposition figures overseas.[24] This aligns with Iran's top priority of regime survival: by hacking email or social media accounts of activists, Iran can identify networks, monitor plans for protests, and possibly disrupt anti-regime activities. The UK is home to a large Iranian diaspora and to a vibrant Persian-language mediin-exile that is often opposed to the Iranian Revolutionary regime. In 2022 the UK government revealed that IRGC-linked agents had not only plotted physical attacks on British-Iranian dissidents, but also engaged in cyber stalking and intimidation – for example, hacking CCTV cameras around a dissident's workplace to track their movements, or flooding their phones with spyware-laced message. Such tactics serve Iran's foreign policy by exporting its repression beyond its borders, signaling to dissidents that nowhere is truly safe.[25] Beyond Iranian targets, Tehran also spies on other communities in Britain that intersect with its interests – for instance, British Jewish organisations (given Iran's hostility to Israel) and Arab dissident circles (e.g. exiled activists from Ahwazi Arab, Iraqi, or Syrian communities). The arrest of Iranian agents in 2023 for surveilling a

[24] UK Parliament, House of Commons Foreign Affairs Committee, *No Protection, No Freedom: The Foreign Policy Implications of the IRGC's Hostile Activities*, HC 313 (2023), 14, https://committees.parliament.uk/publications/40891/documents/199902/default/.
[25] Dan Sabbagh, "Iranian Spy Agents Target Dissidents in UK Using Cyber Surveillance, Says MI5," *The Guardian*, November 16, 2022, https://www.theguardian.com/uk-news/2022/nov/16/iranian-spy-agents-target-dissidents-in-uk-using-cyber-surveillance-says-mi5.

UK-based Israeli target and an attempted plot on an Israeli embassy in London shows how Iran uses espionage (cyber and physical) as a precursor to possible terrorist acts, in line with its goal of confronting Israel even on foreign soil. All of this underscores that the IRGC's cyber espionage is not random – it is carefully aligned with Iran's strategic objectives: keep the regime's enemies (domestic or foreign) under watch, steal anything that can bolster Iran's power, and gather leverage to use in international disputes.

To illustrate, consider the scenario of IRGC hackers obtaining private emails of a UK minister or journalist who advocates tough policies on Iran. Iran could use that information in multiple ways: to quietly inform its diplomacy (knowing the UK's negotiating stance in advance), or to discredit the individual critic by leaking potentially embarrassing intelligence gleaned from the hack. This kind of hack-and-leak tactic was employed by Russia in the 2016 US election and Iran has certainly noticed the impact. IRGC cyber units have already engaged in several such information dumps. In one case, Iranian hackers released the personal data of Iranian opposition members abroad as a means of intimidation. While a large-scale Iranian hack-leak operation against UK figures has yet to occur publicly, the infrastructure and intent are in place. The NCSC explicitly warned in 2023 that these groups seek to *"steal secrets – or leak correspondence to embarrass high-profile figures"*, distinguishing them from ordinary cybercriminals. Thus, surveillance bleeds into covert influence, showing how IRGC cyber espionage directly facilitates information warfare.

Influence, Subversion and Ideological Operations

Perhaps the most insidious way IRGC cyber activities serve Iran's agenda is by shaping narratives and loyalties – influencing foreign populations and undermining social cohesion in adversary countries. Iran's theocratic regime has an ideological mission: to export the Islamic Revolution and champion "resistance" against the West and Israel. The IRGC, as the self-described vanguard of that revolution, is heavily involved in what could be termed *cyber-enabled foreign influence operations*. By disseminating propaganda online and amplifying extremist ideology, the IRGC seeks to extend Iran's ideological reach into communities abroad, including within Britain.

One aspect of this is straightforward state propaganda, using covert Iranian-controlled media to sway public opinion in the UK in directions favourable to Tehran. For example, the fake "news" websites and social accounts run out of Tehran (uncovered by Facebook) pushed content criticizing Western military actions and extolling Iran's allies. This serves Iran's foreign policy by eroding support for Western pressure on Iran and by spreading Iran's narrative on conflicts (portraying, say, Iranian-aligned militias in Iraq or Lebanon as heroic "resistance" and their Western/Gulf opponents as ISIS-sponsors). When British social media users encounter such disinformation – perhaps not realizing its origin – it can subtly shift discourse, injecting Tehran's talking points into debates about Middle East policy, energy security, or Muslim world issues. Over time, this can translate to a more *Iran-sympathetic environment*, which Tehran can exploit diplomatically.

However, the IRGC's influence operations go beyond broad propaganda targeting the UK public at large. A particularly concerning focus is Iran's goal of seeking to export its own revolutionary Islamist world view, and to radicalise British Muslims, both Shia and Sunni. Emotive issues such as Palestine are used to draw individuals into pathways which may result in the abandonment of British values and the adoption of an fundamentalist, revolutionary worldview, support for Iran's transnational agenda (such as backing Hezbollah or opposing Israel and Sunni Gulf states), and potentially the recruitment of operatives or at least sympathisers on UK soil. As will be detailed in the next section, IRGC-linked clerics and centres in Britain have been active in spreading Khomeinist Islamist ideology, glorifying Iran's military leaders, and encouraging communal mobilisation under Iran's banner. This directly serves Iran's foreign policy goal of *"exporting the Islamic revolution"*, by creating nodes of influence in foreign lands. The IRGC's Quds Force (responsible for external operations) explicitly tries to build fifth-column networks among Shia diasporas; for instance, Iran has provided ideological training to foreign recruits at institutions like Al-Mustafa University in Qom, hoping they return to Western countries as its mouthpieces. Cyber and social media play a huge role in this indoctrination pipeline: many younger British Shia or convert Muslims consume Iranian propaganda online (through YouTube sermons, WhatsApp groups sharing IRGC-themed songs, or Twitter accounts praising Iran's Supreme Leader). By these means, the IRGC advances its long-term foreign policy of positioning Iran as the leader of global Islamist resistance, even in the heart of the West.

From the UK perspective, such influence ops are tantamount to subversion. They can incite British Muslims (or even non-Muslim anti-imperialist activists) to take positions hostile to British interests or values. For example, Iran's network in the UK has promoted the narrative that the British government is an enemy of Muslims due to its stance on Israel and Saudi Arabia, thereby widening rifts between British Muslim citizens and their government. Iranian disinformation has also trafficked in conspiracy theories – e.g., blaming MI6 or the CIA for creating ISIS – which, if believed, can radicalise individuals toward Tehran's revolutionary worldview. As one think-tank study puts it, the IRGC is *"nurturing homegrown extremism on UK soil"*, using propaganda much like ISIS or al-Qaeda do. But whereas ISIS propaganda seeks to turn Western Muslims against their governments in a nihilistic jihadist revolt, the IRGC's propaganda seeks to turn them into pro-Iran militants or at least advocates, channeling any anger towards Iran's chosen enemies (Israel, America, Gulf monarchies, or even Iranian dissidents).

Iran's foreign policy benefits from this in multiple ways. It gains soft power and potential hard power assets: a radicalised pro-Iran activist in London might one day help Iran by lobbying politicians, spying on dissidents, or even participating in violence directed by Tehran. Also, by stirring sectarian or political divisions in the UK, Iran distracts and weakens a key Western state. As an authoritarian regime, Tehran takes a cynical view that sowing chaos in liberal societies makes them less effective at countering Iran abroad. Thus, if IRGC-fomented extremist rhetoric in the UK leads to, say, sectarian clashes or public disorder at protests, Iran is quite content to watch Britain grapple with those problems.

In summary, IRGC cyber and influence operations serve Iran's agenda by: (a) Disrupting and deterring adversaries(imposing costs and signaling capability to discourage aggression against Iran), (b) Conducting espionage and surveillance to give Iran strategic advantage and protect the regime (through stolen tech, insight into enemy plans, and monitoring of opposition), and (c) Projecting ideological influence to expand Iran's revolutionary axis and undermine the social stability of its foes. All these outcomes align with the Islamic Republic's long-standing objectives: preserving itself, countering Western influence, and exporting its revolution. The United Kingdom, as a prominent Western power, a close US ally, and home to communities of interest (Iranian exiles, Shia Muslims, etc.), finds itself squarely in Tehran's sights.

We now turn to one of the most sensitive aspects of this threat – the IRGC's impact on Britain's own minority communities and social fabric.

Threat to Arab and Muslim Communities in Britain: IRGC Radicalisation & Disinformation

One of the most troubling dimensions of the IRGC's activities in the UK is the targeted ideological manipulation of British Arab and Muslim communities. Through a network of religious centres, media outlets, social campaigns and covert online influence, the IRGC and its affiliates are attempting to radicalise segments of these communities – disseminating disinformation, sectarian propaganda, and the extremist Islamist ideology espoused by the two clerics who have been the Supreme Leaders of Iran since the 1979 revolution, Ayatollahs Khomeni and Khamenie.

This strategy not only serves Iran's foreign policy (by cultivating support for its agenda in Western societies), but also poses direct risks to the social cohesion and security of the UK. It introduces a toxic foreign extremism into domestic discourse, with the potential to inspire hatred, inter-community tensions, or even terrorism on British soil. In effect, the IRGC is exporting the template of Khomeinist radicalisation – which it has used for decades to indoctrinate fighters in Lebanon, Iraq, and Yemen – into the UK's diaspora context. British authorities are increasingly sounding the alarm: in early 2023, the head of MI5 warned of *"Iranian diplomatic and security channels"* nurturing extremism, and by 2025 the Charity Commission and Home Office were moving to crack down on IRGC-linked community organisations.[26]

An IRGC flag is openly displayed in London during an annual pro-Iran Al-Quds Day rally (2021). Such public demonstrations, organised by IRGC-affiliated networks, show Tehran's ideological reach into segments of Britain's Muslim communities.

[26] Katherine Bauer et al., *Iranian Influence Networks in the West*, The Washington Institute for Near East Policy, Policy Focus 163, March 2020, https://www.washingtoninstitute.org/policy-analysis/iranian-influence-networks-west.

IRGC proxies on UK soil – the “London office” of Iran’s revolution

At the heart of Iran’s influence network in Britain is the Islamic Centre of England (ICE), a Shi’ite religious and cultural centre in Maida Vale, London. The ICE is effectively Iran’s hub for ideological operations in the UK. Its director is directly appointed by Ayatollah Khamenei as his personal representative, and the centre is funded and staffed by individuals tied to the Iranian regime. Alicia Kearns MP, Chair of the Foreign Affairs Committee, has described ICE bluntly as the *“London office of the IRGC,”*and an influential UK think-tank report called it the *“UK nerve centre”* of Iran’s influence network. Under the cover of charity status, ICE has hosted events glorifying IRGC commanders and pushed Tehran’s narratives. In January 2020, just days after IRGC General Qassem Soleimani (leader of the Quds Force) was killed by a US drone, the ICE held a candlelit vigil in his honour in London – publicly mourning a man whom the UK had officially designated a terrorist. At that event, a speaker praised Soleimani as a *“dedicated soldier of Islam”* and celebrated his “martyrdom”. British children from the community were even given special lessons venerating Soleimani as a heroic martyr.

These actions prompted stern rebukes, with the Charity Commission issuing an official warning to ICE for eulogising a terrorist and for failing its duty of balance. Yet the centre persisted in its hardline propaganda. By 2022–2023, ICE’s YouTube channel was found hosting videos of Iran’s Supreme Leader calling Israel a *“cancerous tumour”* that must be eliminated – essentially calling for Israel’s destruction – and promoting conspiracy theories accusing the West of creating ISIS.[27] In May 2025, the Charity Commission concluded ICE had repeatedly spread extremist, anti-Israel material online and was “mismanaged” by allowing this; it issued a rare Section 84 order compelling ICE’s trustees to curb all such content and vet speakers going forward. Notably, the Commission’s investigation explicitly cited allegations that ICE *“was the London office of the IRGC”* as part of its rationale. In other words, the UK government regulator recognises that ICE has been acting less as a benign cultural charity and more as an outpost of Iranian state indoctrination on British soil.[28]

ICE is not alone. At least half a dozen mosques and religious centres across the UK have been identified as part of the pro-Iran network. Many of these hosted memorials or celebrations for IRGC “martyrs” like Soleimani in early 2020. They invite clerics closely linked to the Iranian regime to speak. Some of those clerics preach in Urdu or Arabic to connect with South Asian and Arab Shia communities in Britain, extending Iran’s reach beyond Persian-speaking circles. An example is the *Hussaini Islamic Mission* in Manchester, which reportedly held events praising Iran’s leadership. These centres often have social media pages where they share IRGC propaganda videos and statements from Khamenei.

---

[27] Jewish Chronicle, “Charity Commission Investigates Mosque over Khamenei Videos Calling for Israel’s Destruction,” *The Jewish Chronicle*, March 10, 2023, https://www.thejc.com/news/news/charity-commission-investigates-mosque-over-khamenei-videos-calling-for-israels-destruction-5y2e6h9c.

[28] Charity Commission for England and Wales, *Official Warning to the Islamic Centre of England Ltd*, May 2023, https://www.gov.uk/government/publications/official-warning-to-the-islamic-centre-of-england-ltd.

Radicalisation of youth – “Soldiers” of the Hidden Imam in London

Perhaps the most striking example of IRGC ideological penetration in Britain is the “Salute Commander” video produced in mid-2022. “Salute Commander” is an Iranian propaganda song that calls on children to pledge allegiance to the 12th Imam (a messianic figure in Shia Islam) and to be ready to fight in apocalyptic battles preceding his return. It was heavily promoted by IRGC media inside Iran. Astonishingly, an *official music video in English was recorded on UK soil* for this song. The filming took place at two Tehran-linked sites in London: the Islamic Republic of Iran School in Kilburn (which is run by the Iranian embassy) and the ICE in Maida Vale. The video shows a group of children – British Shia youths of various ethnic backgrounds – singing in unison that they will join the 313 special fighters of the Mahdi (the prophesied saviour) and expressing a wish to become “martyrs”. Clad in white, the children chant lines like *“Do not see me as too young… I’ll answer the call”*, while performing salutes. They explicitly pledge loyalty to Ayatollah Khamenei as part of this militant devotion.[29]

A still from the “Salute Commander” video, recorded in London (2022), shows young children pledging readiness to fight and die at the behest of Iran’s Supreme Leader. Such IRGC-sponsored content illustrates the indoctrination of diaspora youth with extremist ideology.

[29] Jake Wallis Simons, “British Children Filmed Singing ‘We Are Ready to Be Martyrs’ for Iran’s Supreme Leader,” *The Jewish Chronicle*, July 28, 2022, https://www.thejc.com/news/news/british-children-filmed-singing-we-are-ready-to-be-martyrs-for-irans-supreme-leader-3p3qafpj.

The content of the song and video is deeply ideological: it ties the religious concept of the Mahdi's return to modern political allegiance, effectively telling children that following Iran's Supreme Leader and fighting his enemies (e.g. Israel, the West) is a divine duty. That this was staged in London – with British-Iranian children – is a chilling indicator of IRGC indoctrination efforts inside the UK. It suggests the IRGC has successfully cultivated a support base to the extent of getting minors to glorify jihad on camera. UK observers were alarmed; counter-extremism experts noted that this mirrors how ISIS and other jihadists groom children, albeit in a Shia revolutionary context.

The presence of an IRGC-affiliated video production in the UK prompted calls for stronger action. Analysts argued this demonstrated a homegrown extremist base linked to Iran, and that Britain's *Prevent* programme (which combats radicalisation) should broaden beyond Sunni extremism to also address "Shia Islamist extremism" propagated by Iran. The fact that these children could be mobilised for a slick video also raises fears about what else they could be mobilised for in the future, if Iran called on its devotees.[30]

[30] Jake Wallis Simons, "Iranian School in London That Sparked Antisemitism Fears Served with Enforcement Notice," *The Jewish Chronicle*, February 24, 2023, https://www.thejc.com/news/news/iranian-school-in-london-that-sparked-antisemitism-fears-served-with-enforcement-notice-1N0XK0AFiGy1DhplKLgrR8.

Sectarian and ideological influence

The IRGC's outreach in Britain primarily targets Shia Muslim communities (of Iranian, Iraqi, Pakistani, and Lebanese heritage), as they are seen as natural constituencies for Iran's Islamist revolution. However, Iran also seeks to influence wider Muslim and Middle Eastern diaspora debates by positioning itself as the champion of anti-Zionism and anti-imperialism. One method is sponsoring the annual *Al-Quds Day* march in London – a protest against Israel's control of Jerusalem, initiated by Ayatollah Khomeini. UK observers note that Al-Quds Day events in London often feature Hezbollah flags and portraits of Khamenei or IRGC generals, carried by some participants. These rallies, organised by groups like the Islamic Human Rights Commission (IHRC, a UK charity with Iran-friendly leanings), serve as visible propaganda for Iran's cause. They also can intimidate British Jewish communities (hence undermining interfaith relations) when protesters call for "death to Israel" on the streets of London. The IRGC's hand is indirect but discernible – Iranian state media eagerly cover these UK rallies, portraying them as evidence that "the Muslim ummah in the West" supports Iran's anti-Israel stance. Such imagery aligns with Iran's foreign policy goal of rallying the Muslim world around the Palestine issue (with Iran at the helm).[31]

The IRGC's influence can create or exacerbate sectarian tension between different British Muslim groupings. Iranian propaganda in Arabic and Urdu sometimes contains anti-Sunni rhetoric or glorifications of Shia militia (such as Iraq's Hashd al-Sha'bi or Yemen's Houthis) that Sunni Muslims view with hostility. The Policy Exchange think-tank recently highlighted that London is now host to pro-Iran activists including some linked to *Hashd al-Sha'bi militias*, and warned that *"Iran and its supporters have sought to influence protests… which are likely to negatively impact UK social cohesion."*. An example was during the May 2021 Israel-Gaza conflict: pro-Palestinian demonstrations in Britain saw the presence of Iranian flags and slogans in support of Hamas/Hezbollah. While most protestors were not Iran-aligned, even a small contingent visibly pushing Tehran's line can stoke concerns (the UK police noted some protesters bore imagery of banned Hezbollah). By inserting itself into these volatile events, the IRGC network takes advantage of genuine grievances to push a more extreme narrative, potentially radicalising a minority of participants towards militancy.

Threats to dissidents and minorities

Another facet of the IRGC's threat to communities in Britain is direct intimidation of Iranian dissidents, as mentioned earlier, and of other anti-Iran regime minorities (such as Ahwazi Arabs, Kurds, or Balochis living in the UK). The IRGC and Ministry of Intelligence have attempted to silence many such critics, here in Britain, through cyber-harassment, and have even plotted their assassination/kidnapping. This creates a climate of fear in those diaspora communities, and a severe infringement of their freedoms and security. British-Iranian journalists have had to relocate their homes and

[31] Katherine Bauer et al., *Iranian Influence Networks in the West*, The Washington Institute for Near East Policy, Policy Focus 163, March 2020, https://www.washingtoninstitute.org/policy-analysis/iranian-influence-networks-west.

some now live under armed guard. Such activities directly threaten the targeted communities and violate UK sovereignty, and create a climate of fear and mistrust which pervades all aspects of communal and personal life.

In summary, the IRGC's outreach into Britain's Arab and Muslim communities is a strategic effort to entrench the Islamic Republic's ideological influence within the UK. By embedding its narratives in diaspora spaces—through disinformation, sectarian messaging, and religious propaganda—the IRGC seeks to cultivate sympathetic networks abroad and export its revolutionary doctrine. This is not merely a cultural export but an ideological penetration with tangible consequences for both the targeted communities and wider British society.

For Britain's Arab and Muslim communities, the consequences are twofold. First, the exposure to extremist narratives—including anti-Western, antisemitic, and sectarian content—risks undermining community cohesion and promoting radicalisation. Second, these same communities may become unwitting collateral, either by being stigmatised or mischaracterised as "fifth columns" or by drawing the attention of law enforcement and counterterrorism services.

The broader societal impact is also deeply concerning. Iran's slow-burning information warfare strategy poses a corrosive threat to social cohesion. Unlike the immediate shock of a cyberattack or assassination plot, this campaign operates subtly—through sermons, youth activities, online propaganda, and religious centres—to reshape identities and allegiances, especially among younger generations. Its goal is to erode the norms of integration and pluralism, replacing them with ideological loyalty to Tehran and its Supreme Leader.

UK security services now publicly acknowledge the severity of this challenge. MI5 and Counter Terrorism Police have reportedly increased surveillance of Shia religious centres and charities with suspected links to Iran. Legislative proposals have been floated to criminalise collaboration with hostile state actors—including the IRGC—with penalties of up to 14 years in prison. These legal steps reflect a growing awareness that Britain's legal and cultural openness is being exploited by an adversarial power to wage psychological and ideological warfare on home soil.

This campaign, if left unchecked, could undermine Britain's hard-won efforts to promote interfaith harmony, counter violent extremism, and maintain an inclusive national identity. The IRGC's attempt to build a psychological and ideological bridgehead in the UK must be treated not merely as a foreign policy concern, but as a domestic security and social integrity issue. A policy response must be holistic, combining proscription, community engagement, and the strengthening of counter-extremism frameworks to address this unique and insidious threat.

Strategically, countering this will require not only security measures but also community engagement to expose and refute Iran's propaganda. The next section will address policy responses, foremost among them the long-awaited step of banning the IRGC outright.

Strategic and Policy Recommendations for the UK

Confronted with the IRGC's multidimensional cyber threat – encompassing espionage, sabotage, disinformation, and extremist radicalisation – the United Kingdom must respond with equal breadth and determination. The evidence is overwhelming that Iran's Revolutionary Guard is operating as a hostile actor on UK soil and in UK cyberspace, in many ways mirroring the behavior of proscribed terrorist organisations. Indeed, the IRGC's blend of cyber attacks, assassination plots, and extremist propaganda shows it *"operates no differently to proscribed groups… including ISIS, al-Qaeda and Hezbollah,"* as one briefing to Parliament observed. Yet, unlike ISIS or al-Qaeda, the IRGC still is not banned in the UK as a terrorist entity – a loophole that Iran has exploited to expand its networks with relative impunity. This needs to change. Below are strategic and policy recommendations to mitigate the IRGC's threat, centered on the necessity of proscribing the IRGC and accompanied by further measures in cybersecurity, law enforcement, community protection, and international coordination. These recommendations are aimed at UK lawmakers and security officials, and are grounded in the principle that a comprehensive response – treating the IRGC as the terrorist-paramilitary organisation that it is – will strengthen Britain's national security and resilience.

Proscribe the IRGC under UK Terrorism Laws (with urgency and robust implementation)

The single clearest step is to formally ban the IRGC as a terrorist organisation, as has been repeatedly advocated in Parliament (including a unanimous Commons vote in January 2023).

Proscription would make it a criminal offense to belong to the IRGC, attend its meetings, or publicly support it, and would empower authorities to seize IRGC-related assets. This sends a powerful message of zero tolerance. As the Tony Blair Institute argued, *"Formally banning the IRGC will send a clear message to the clerical regime in Iran that the terrorism and militancy pursued through the Guard, including on UK soil, will not be tolerated."* It would put Iran's leaders on notice that their elite unit's activities in Britain are beyond the pale.[32]

[32] Tony Blair Institute for Global Change, *Time to Proscribe: Why the UK Government Should Ban Iran's Islamic Revolutionary Guard Corps*, January 2023, https://institute.global/policy/time-proscribe-why-uk-government-should-ban-irans-islamic-revolutionary-guard-corps.

Crucially, proscription is not merely symbolic. It creates legal teeth: any UK-based charities, centres or individuals proven to be directing support to the IRGC or coordinating with it could face arrest and prosecution. For instance, if IRGC were banned, the Islamic Centre of England's alleged role as the IRGC's "London office" would be untenable – any coordination or direction from IRGC to ICE staff could trigger terror charges.

The UK has already sanctioned the IRGC in its entirety, which freezes its assets.Proscription goes further, by criminalising interaction. One proposal from the Home Office is to use new powers so that *"anyone helping or benefiting from a banned state intelligence agency"* (such as the IRGC) faces up to 14 years imprisonment. This would let MI5 and police clamp down on IRGC agents or recruiters operating in the UK in a way they currently cannot.

It bears noting that the IRGC easily meets Britain's legal criteria for terrorism: it engages in *"serious violence against persons"* (as seen in its overseas plots) and *"serious damage to property"* for political ends (e.g. its cyber sabotage) to intimidate governments – all hallmark terrorist behavior. Countries such as the United States, Canada, and many of Iran's neighbors have already designated the IRGC as a terrorist group. The UK should join their ranks, eliminating the current inconsistency whereby Hezbollah is banned in the UK while its creator and funder (the IRGC) is not.[33]

In implementing proscription, the government must be prepared to follow through robustly. A "whole-of-government" approach should accompany the ban: intelligence agencies ramping up surveillance on IRGC-linked entities, the Charity Commission intensifying oversight of Shi'ite charities (to ensure they are not fronts for IRGC extremism), and the Crown Prosecution Service readying cases where appropriate. To prevent proscription from being a mere *"glass ceiling"* – a formal ban with little practical effect – it should act as *"a spur for further action,"* as recommended by Policy Exchange. This includes updating guidance so that any *"contact between [the IRGC] and British citizens is effectively criminalised."* For example, Britons who travel to Iran for paramilitary training or who disseminate IRGC propaganda could be prosecuted analogously to how those aiding ISIS were. Proscription will also aid tech companies and civil society: it would give a clear mandate to social media platforms to remove IRGC-affiliated content and accounts (which they would be able to justify under UK law as terrorist material), and to community leaders to reject IRGC-linked partnerships. Notably, banning the IRGC does *not* preclude diplomatic engagement with Iran's civilian government on urgent issues, just as banning Hezbollah did not halt UK ties with Lebanon's government. It simply draws a red line around the IRGC's militant activities.

[33] U.S. Department of State, "Designation of the Islamic Revolutionary Guard Corps," April 8, 2019, https://2017-2021.state.gov/designation-of-the-islamic-revolutionary-guard-corps/index.html.

Enhance Cyber Defense and Intelligence-Sharing Focused on Iran

On the cyber front, the UK should boost its defensive measures and international cooperation specifically against Iranian cyber threats. The NCSC, working with GCHQ, should continue to issue public advisories about Iranian cyber tactics (as it did in 2023 regarding spear-phishing), and to help UK institutions to harden their email security and to train staff to spot impersonation attempts. Given that Iranian hackers often target academia and think tanks, the NCSC might establish a special outreach program to universities and research institutes – offering assistance in protecting sensitive research and student data (building on lessons from the Mabna hacks).

The UK should also leverage the “Five Eyes” and EU partners for threat intelligence on Iran. Joint cybersecurity advisories like the December 2024 alert co-authored by NCSC, CISA, NSA, and others about IRGC PLC attacks have been very useful. Continued intelligence-sharing will ensure Britain is aware of new Iranian malware or phishing campaigns in real time. As Iran incorporates AI into its cyber ops, the UK’s cyber analysts must stay ahead with predictive models and by tapping industry expertise (e.g. collaborating with cybersecurity firms that track Iranian APTs, such as Recorded Future, Mandiant, etc.).

UK agencies should also consider proactive cyber measures to deter Iran, even moving towards a footing that might be described as being ‘on the offensive’. Measures could range from quietly neutralising Iranian command-and-control servers targeting UK infrastructure, to exposing IRGC hackers’ identities publicly (as the US FBI has done via indictments). Such “naming and shaming” can create real costs for IRGC agents, either financial or by creating frictions and constraints, such as on international travel, which impede their abilities to operate. The UK should also coordinate closely with other nations who are frequently hit by IRGC cyber attacks, such as Israel and the Gulf states, as these allied powers will have defensive tools and strategies that can bolster UK preparedness. Israel, for example, has had to act to protect its vital civilian infrastructure, notably its national water system, from Iranian cyber attacks, and could help the UK climb the learning curve more rapidly and with less risk than doing it alone.

On the policy level, Britain might push for multilateral frameworks that hold Iran accountable – for instance, using the UN or European bodies to condemn state-sponsored cyberattacks (similar to how North Korea’s WannaCry was internationally attributed). While Russia often shields Iran diplomatically, building a consensus among Western and allied states that Iran’s cyber aggression is unacceptable could lay groundwork for future sanctions or responses.

Crack Down on IRGC Networks and Fronts in the UK (Beyond Proscription)

Proscribing the IRGC needs to be the first step in a campaign to actually uproot the IRGC's penetration of, and influence nm Britain. UK authorities will have to intensify the monitoring and regulation of institutions tied to Iran's regime, and will have to be prepared - if necessary - to close down any institutions that do not comply with the law.

The Charity Commission should be commended for finally taking action on the Islamic Centre of England – but it is likely to need more resources, more powers, and strong backing from the Government to ensure it can tackle such cases swiftly. One recommendation is to bar known IRGC operatives or Iranian regime clerics from entering the UK. Refusing to grant such individuals an entry visa is justified due to the risk that they might spread extremism and damage social cohesion. The Policy Exchange report *"Tehran Calling"* suggests the Home Office issue an order denying entry to any individual employed by Iranian state religious bodies (like Al-Mustafa University) who doesn't pass a strict extremism test. Stopping the revolving door of hardline Iranian preachers visiting UK mosques to propagate Tehran's ideology is an eminently attainable policy objective.

MI5 and counter-terror police should prioritise infiltration and surveillance of IRGC-linked networks domestically. This might involve undercover work in community centres or monitoring of flows of money from Iran to UK-based organisations. Any entities found funneling Iranian state funds for unlawful purposes should have their assets frozen or be shut down. The UK's 2023 decision to open an investigation into ICE was a good start; that inquiry must now be seen through to resolution, and its practices applied to other charities with similar levels of association with the Iranian regime and IRGC. The Charity Commission should move to the front foot in replacing the trustees of these charities with an interim manager (as the Charity Commission already did with ICE) and even deregistering the charity if non-compliance continues. The same scrutiny should apply to other Iran-linked charities or media outlets. Ofcom and online regulators should ensure Iranian state media content (e.g. Press TV's online broadcasts) is not violating UK laws on hate speech or incitement; if they are, access from the UK should be blocked and social media companies should remove their accounts.

Moreover, to address disinformation, the UK might consider creating a dedicated Foreign Influence Taskforce (similar to units in the US and Australia) that identifies and counters malign foreign influence campaigns. Iran should be one of its focus areas, alongside Russia and China. This taskforce could work with social media platforms to rapidly take down fake profiles tied to IRGC propaganda (like those Facebook removed), and to push truthful counter-messages in communities targeted by Iranian

propaganda (for example, providing factual rebuttals to Iranian conspiracy theories in Arabic or Farsi on diaspora forums).[34]

Protect and Empower At-Risk Communities, Counter-Extremism in New Domains

The UK should simultaneously inoculate vulnerable communities from IRGC radicalisation. Specifically, we call for the UK Government to expand the Prevent programme's scope to include Shia Islamist extremism. Prevent officers and local authorities could engage Shia community leaders and youth groups, raising awareness that Iranian regime propaganda is manipulative and not representative of British Shia values. Educational initiatives can be launched, for example, to help parents understand why letting their child participate in an IRGC video or chant about martyrdom is harmful – analogous to how families are cautioned about ISIS grooming. Scholarships or support for independent Shia religious education (free from Tehran's influence) could be considered, to offer an alternative to IRGC-funded narratives. The government might facilitate a forum of British Shia scholars and imams who reject Khamenei's politicised Islam, amplifying their voices as a counterweight to the Iran-aligned preachers.

Arab Sunni communities in the UK, who might consume Iranian disinformation on Middle East issues, also need resilience training. Civil society groups can help fact-check and debunk viral falsehoods coming from Iranian sources – for instance, Iran's state media often spreads fake news about Western plots against Muslims. Community media and mosques should be equipped with accurate information to counter these. Interfaith and inter-sect dialogue can mitigate the sectarian poison Iran tries to inject: if British Sunnis and Shias see each other as partners, it blunts Iran's attempt to rally Shias in a zero-sum cause.

Importantly, protecting British-based Iranians, especially those perceived as anti-regime dissidents, must be a priority. The UK should continue providing enhanced security (police details, alert systems) to Iranian dissident journalists and activists under threat. The IRGC has shown it will stop at nothing, even attempting kidnappings in London suburbs. Iranian expats fearing persecution for online speech should be recognised as likely to qualify for asylum in the UK, and fast-track procedures should be established to grant them refugee status. This accords with existing Home Office's guidance, which already suggests that those targeted by Iran's cyber-surveillance may qualify for asylum. By giving safe haven to Iranian dissidents,, the UK denies Iran the success of silencing its critics.

[34] essica Brandt and Bret Schafer, *Countering Foreign State Propaganda and Disinformation in the Digital Age*, Brookings Institution, April 2020, https://www.brookings.edu/articles/countering-foreign-state-propaganda-and-disinformation-in-the-digital-age/.

International Pressure and Diplomacy Focused on IRGC Behavior

Finally, the UK should work with allies to increase international pressure on Iran specifically over IRGC malign activity. While Iran's nuclear ambitions often dominate the international community's diplomatic agenda, Britain can use its platform at the UN and its many strong bilateral relationships to highlight IRGC cyber-attacks and transnational repression. The UK should make the case for a UN Special Rapporteur report, or for a NATO/EU statement, that catalogs Iranian cyber aggressions (much as has been done for Russian cyber ops). Publicly attributing attacks to IRGC (when evidence allows) strips away their deniability. The UK could also consider tying any future improvements in UK-Iran relations to a scaling back of IRGC hostile activities: for example, conveying to Tehran that there will be no restoration of full diplomatic ties or sanctions relief as long as the IRGC (or its cut-outs) continue to plot assassinations in the UK or hack British institutions. In essence, create conditionality whereby improvements in relations between Iran and the international community are explicitly tied to the IRGC's conduct.

Britain should also coordinate sanctions with allies. If the IRGC cannot yet be globally banned (due to some countries' objections), targeted sanctions on IRGC cyber units and front companies can be expanded. The US has sanctioned entities like the Mabna Institute and individuals including IRGC hackers; the UKand Europe can mirror these actions so that IRGC cyber operatives cannot travel or do business in our neighbourhood. Additionally, pressing allied Arab powers, such as Iraq and Lebanon, to deny IRGC operatives freedom of movement can reduce the IRGC's ability to run networks that might reach into Europe.

To counter the threat of IRGC-sponsored radicalisation of British muslims, the UK should also leverage its relationships with neighbouring European powers, and friendly muslim-majority powers (notably the Gulf states), Together, educational and religious resources can be created and promoted to expose Iran's mis-use of is using religious programming to indoctrinate diaspora youth, and to ensure that lessons learned from countering new IRGC-tactics in any one country are rapidly shared with others likely to be targeted by similar tactics in short order. Demonstrating a united front against IRGC actions would have a powerful inhibiting effect, but would require a consistent, concerted and high-profile effort from the UK and allied governments.

Conclusion

The IRGC's cyber threat to the United Kingdom is not a remote or hypothetical danger – it is here and now, spanning the digital and physical realms. From hacking university databases to inciting British children to pledge martyrdom for Iran, the IRGCpresents an assault on the UK's security, sovereignty, and social harmony by an organ of a foreign power.

UK legislators and authorities must now publicly recognising the IRGC for what it is: a state-run terror-insurgency organisation with global reach.

The UK's policy response must therefore be bold and unambiguous. Proscribing the IRGC will lay down a firm marker and unlock stronger enforcement against its networks. But proscription is only the first step. Britain must also harden its cyber defenses, root out IRGC influence in communities, punish acts of cyber aggression, and lead international efforts to hold Iran to account.

This multi-pronged strategy, grounded in vigilance and the rule of law, will significantly constrain the IRGC's ability to menace the UK. As one briefing aptly noted, *"The IRGC fits all the criteria for proscription… [Its] surge in activity on UK soil, including foiled terror plots and assassination attempts [in 2022], makes action more important than ever."*

Britain is facing an adversary that respects no boundaries in pursuit of Tehran's extremist goals, and so Britain must draw clear lines to protect what is precious from those who wish to do us harm. By doing so – by declaring that Iran's Revolutionary Guard and its cyber warriors are persona non grata in the United Kingdom – the UK will not only protect its national interests but also stand in solidarity with the Iranian people who suffer under the IRGC's oppression. It will be a clear, incisive stance in defense of democracy and security against a growing cyber-espionage empire. The time to act is now, with strength and strategic clarity, to ensure the IRGC's dark web of influence finds no sanctuary in Britain.