

Presented by WBII

# PARLIAMETARY BRIEFING

The IRGC in Britain's  
Digital Backyard: A  
Strategic Threat to UK  
Security and Social  
Cohesion

JUNE 2025



FORUM FOR  
FOREIGN  
RELATIONS



GPS



[advocacy@webelieveinisrael.org.uk](mailto:advocacy@webelieveinisrael.org.uk)



[www.webelieveinisrael.org.uk](http://www.webelieveinisrael.org.uk)



**A new in-depth policy briefing from the Forum for Foreign Relations, The IRGC's Cyber Threat to the United Kingdom, details how Iran's Islamic Revolutionary Guard Corps (IRGC) has evolved into a formidable cyber and ideological threat within Britain. No longer confined to regional proxy warfare, the IRGC today engages in digital sabotage, information warfare, and ideological subversion on UK soil — including attacks on parliament, universities, critical infrastructure, and diaspora communities.**

**Despite growing evidence of IRGC activity within the UK, the organisation remains unproscribed, limiting the government's ability to respond to these provocations with full legal and operational authority. This briefing outlines key findings from the FFR report and urges Parliament to act decisively.**

## Key Findings

- **Cyber Intrusions on British Institutions**
- **The IRGC and affiliated hacker groups (APT35, MuddyWater, Mabna Institute) have:**
  - Breached UK parliamentary email systems, including MPs’ accounts (2017).
  - Conducted credential theft targeting British academics, think tanks, and political analysts.
  - Targeted critical infrastructure (e.g., water treatment PLCs) in cyber campaigns linked to IRGC propaganda operations.
- **Targeting British Dissidents and Iranian Exiles**
  - MI5 revealed in 2022 that at least 10 assassination/kidnap plots were linked to Iran in a single year.
  - British-Iranian dissidents have faced cyberstalking, spyware attacks, and physical surveillance — including IRGC agents hacking local CCTV systems.
- **Ideological Manipulation of British Muslim Communities**
  - IRGC-linked networks exploit UK-based charities and schools to disseminate sectarian propaganda.
  - In 2022, the “Salute Commander” video was filmed in London, showing children pledging allegiance to Iran’s Supreme Leader and martyrdom.
  - Al-Quds Day rallies, often featuring Hezbollah flags and chants of “Death to Israel”, are used by Iran-linked organisations to intimidate Jewish communities and spread extremism.
- **Weaponisation of UK’s Academic and Charitable Sectors**
  - The Mabna Institute breached over 300 universities worldwide, including many in the UK, stealing intellectual property for the IRGC.
  - The Islamic Centre of England (ICE), under Charity Commission investigation, has been linked to IRGC messaging and broadcast material promoting Khamenei’s antisemitic rhetoric.
  -

## Recommendations

1. **Proscribe the IRGC in Full under the Terrorism Act 2000**
  - Partial designation (e.g., of the Quds Force) is no longer sufficient. Full proscription would give law enforcement the tools to dismantle domestic IRGC networks and prosecute supporters.
2. **Audit and Regulate IRGC-Linked Charities and Cultural Institutions**
  - Urge the Charity Commission and Home Office to increase scrutiny of organisations tied to the Islamic Republic and its proxies.
  - Ensure funding, activities, and foreign affiliations are transparent and compliant with UK law.
3. **Enhance Cyber Countermeasures and Academic Resilience**
  - Support new NCSC-led initiatives to shield UK universities and think tanks from foreign state-sponsored cyber theft.
  - Provide security briefings and support to individuals and organisations likely to be targeted.
4. **Strengthen Community Resilience to Foreign Extremism**
  - Provide civil society groups and local councils with tools to counter radicalisation and foreign propaganda, especially in minority communities.
  - Publicly affirm support for British Muslims, Arabs, and Iranians targeted by IRGC disinformation and coercion.
5. **Public Inquiry into Iran’s Influence Operations in the UK**
  - Consider launching a formal parliamentary or intelligence-led inquiry into foreign influence campaigns, disinformation networks, and the erosion of UK civil space by the IRGC and its affiliates.

The IRGC poses a clear and escalating threat to UK national security, democratic institutions, and interfaith relations. Its hybrid warfare model — combining cyber aggression, surveillance, radicalisation, and propaganda — operates well beyond Iran’s borders. The United Kingdom must act urgently and decisively by proscribing the IRGC and closing down the domestic networks that sustain its influence.

**For further information, or to receive the full report, please contact:**

**Catherine Perez-Shakdam**  
**Executive Director, We Believe in Israel**  
**Founder, Forum for Foreign Relations**

 [cat@webelieveinisrael.org.uk](mailto:cat@webelieveinisrael.org.uk) |  [www.forumforforeignrelations.org](http://www.forumforforeignrelations.org)