Iran's Shift from Soft to Hardened Targets: Preliminary Observations from the RAF Fairford Incident

By Crispin Smith and Matthew Levitt

Recent Iran-linked plots against U.S. military bases in the United Kingdom highlight a consequential expansion of Tehran's covert campaigns using disposable criminal proxies in Europe. The Islamic Revolutionary Guard Corps (IRGC) and Iranian intelligence services now appear willing to extend this approach beyond dissidents, Jewish communities, and other civilians to hardened military targets. Drawing on official statements, court allegations, public reporting, and author interviews, this article examines the RAF Fairford incident, allegedly orchestrated by individuals behind European bombings earlier in 2026 claimed by Harakat Ashab al-Yamin al-Islamiya (HAYI), an IRGC-linked front. They include Mohammed Baqer al-Saadi, previously profiled in *CTC Sentinel* and awaiting trial for terror offenses in U.S. custody. The article situates both campaigns within Iran's evolving external operations, assesses the strategic implications of increasingly ambitious Iranian-directed proxy attacks, and offers preliminary analysis of the underlying role of various Iranian intelligence organizations. Notably, Fairford illustrates how inexpensive proxy activities can prompt military redeployments, strain counterterrorism resources, and generate friction between allies without causing direct damage. Arresting replaceable recruits alone cannot resolve this challenge. Effective responses should combine protective security and investigations tracing networks to their sponsors with credible financial and diplomatic pressure, stronger deterrence against proxy recruitment, and, where legally justified, targeted military action against overseas handlers directing attacks.

In the small hours of Sunday, September 27, 2026, British counterterrorism police descended on Whelford, a tiny and bucolic village nestled in England's Cotswolds region. Responding to reports of suspicious activity involving men in vans, police detained five men in their twenties near Royal Air Force Fairford (RAF Fairford).

These event caused immediate alarm, since Whelford's picturesque setting belies its strategic import: Its little houses sit just a few hundred feet from the eastern perimeter fence of RAF Fairford, an airbase operated by the U.S. Air Force and its only bomber forward operating location in Europe,[a] supporting aircraft such as the B-1B Lancer, B-2A Spirit, and B-52H Stratofortress.[b]

But though initial reports appeared convoluted and chaotic, the incident has now been attributed to Iranian intelligence operatives[c] including several men linked to the Islamic Revolutionary Guard

Crispin Smith is an attorney based in Washington, D.C., specializing in national security law. His research focuses on operational issues related to irregular warfare, information operations, and lawfare. He directs an initiative designed to counter human rights abusers, foreign terrorist organizations, and hostile states through targeted investigations, and is an advisor on economic and legal warfare at the Irregular Warfare Initiative. Previously, he co-founded the MilitiaSpotlight platform.

Dr. Matthew Levitt is the Fromer-Wexler senior fellow and director of the Reinhard program on counterterrorism and intelligence at the Washington Institute for Near East Policy. Levitt teaches at Georgetown and Pepperdine Universities. He is the author of Hezbollah: The Global Footprint of Lebanon's Party of God *and the creator of interactive, open-access online maps of Hezbollah and Iranian worldwide operational activities. He has written for* CTC Sentinel *since 2008. X: @Levitt_Matt*

© 2026 Crispin Smith, Matthew Levitt

a The United Kingdom has had U.S. forces stationed in the United Kingdom since the Second World War. The United States Visiting Force (USVF) is in the United Kingdom at the invitation of the UK Government. The overarching agreement setting out this relationship is the Churchill–Truman Communiqué of 1952. Forces are governed by the NATO Status of Forces Agreement (SOFA), the Visiting Forces Act 1952, and further bilateral agreements between the United Kingdom and United States, some of which are classified. As of January 2026, there were approximately 11,000 U.S. military personnel permanently based at various locations throughout the United Kingdom. According to the UK Parliament, RAF Fairford is a NATO-designated standby deployment and U.S. forward operating base for US Global Strike Command. It has been used extensively by U.S. military aircraft in previous conflicts, including Operation Iraqi Freedom in 2003. A U.S. Air Force officer, usually of the rank of Colonel, commands U.S. bases in England with a British Royal Air Force commander also present and normally of the rank of squadron leader. See "Research Briefing - US military forces in the UK: Legal agreements," UK House of Commons Library, March 2, 2026.

b In a 2022 interview, a USAF base commander stated "Fairford's in this unique position where we're … the only bomber forward operating location in Europe … [s]o what that means is that we're organized, manned, trained, [and] equipped to support that bomber fleet, both with the necessary specialized ground equipment and the facilities they use, if they need to stand up the mission planning cell or put their maintenance in, because we're not a main operating base. So we're kind of postured here, and that really is our mission, to be ready to support the deploying units here." See Greg Hadley, "RAF Fairford Grows to Support Bomber Task Forces and More," *Air & Space Forces Magazine*, July 29, 2022.

c In a Q&A session with journalists, MI5 Director Ken McCallum said "the RAF Fairford incident, which I won't get further into for reasons you will understand, is not unique … There have been other examples not just in the UK but around the world, including more specifically in Iran's own region." Margaret Davis, "Iran-linked incident at RAF Fairford 'not unique', spy chief says," Press Association, published by *The Irish News*, October 13, 2026.

Corps (IRGC) and believed to also be behind a prior spate of bombings and arson attacks in the United Kingdom and continental Europe in March and April.[1] On October 27, two British men were charged with separate offenses concerning assistance to a foreign intelligence service and activity near a prohibited site,[2] and on November 10, the U.S. Department of Justice unveiled new charges against three Iranian and Iraqi men[3]—including Mohammad Baqer al-Saadi, an IRGC and Kata'ib Hezbollah (KH)-linked operative currently in U.S. custody awaiting trial for federal terrorism charges, and profiled in a May 2026 *CTC Sentinel* by one of the authors (Smith).[4] Al-Saadi and his Iran-based associates now are not only accused of orchestrating the arson and bombing campaign earlier this year, but also of coordinating the RAF Fairford incident.[5]

Concerningly, this campaign of incidents follows growing Iranian hostile activity in Europe, North America, and Australia, including assassination plots, arson, sabotage, and other hybrid activities designed to sow terror, cow regime critics, influence Western governments, and impose costs. Iran is ever more reliant on covert networks and proxies recruited from criminal groups, vulnerable individuals, and lone actors online.[6] The RAF Fairford allegations now describe overseas handlers using local intermediaries to facilitate payments, local logistics, recruitment, and reconnaissance—familiar typologies of the Quds Force (IRGC-QF) and IRGC Intelligence Organization (IRGC-IO), and similar to the European campaign earlier in the year that had primarily targeted Jewish civilian targets like community centers and ambulances. But despite matching patterns of recruitment and control, this latest example suggests a move toward criminal-proxy-delivered effects against a newer type of target: a European military location, harder and of greater strategic import than targets of past efforts.[7]

The activities also reveal important points about Iranian strategy and capabilities. Reliance on proxies suggests an inability to impose costs more directly on Western adversaries. Yet, recruiting and manipulating local individuals to attack increasingly significant targets at low cost presents serious counterterrorism challenges. Meanwhile, the RAF Fairford incident in particular has—whether by accident or design—produced several strategic wins for Iran: the withdrawal of U.S. strategic bombers, allegedly because of Iranian threats;[8] the costs of investigating and prosecuting likely low-level recruits;[d] Anglo-American friction; and local discontent about hosting American bases.[9] Absent significant costs, Iran's security services will likely pursue ever more ambitious proxy-led attacks.

This article will proceed by first setting out the public facts about the plot, the planners' role in prior attacks, and Iran's involvement (Part I). It will then situate the case within Iran's tactical shift toward the use of criminal proxies for strategic "direct action" against both soft and hard targets in the West (Part II), and consider the strategic potential of this approach (Part III) before noting considerations for responding to further incidents (Part IV).

The RAF Fairford Incident: Facts and Assessment

Public facts about September 27 remain incomplete, but official statements, the October 27 English court hearing, and a U.S. Department of Justice indictment unsealed on November 10 permit an increasingly detailed account. Meanwhile, comparisons with earlier Iranian operations, and especially the campaign of bombings and arson attacks carried out earlier this year, also allow some assessments of the plot's development.

Prior to the Incident (March-September 2026)

According to U.S. officials who briefed *The New York Times*, in mid-September commanders received warnings from American and other Western intelligence agencies that RAF Fairford was the target of a potential Iran-backed attack.[10] The warnings drew on intercepted communications, informants, and other intelligence, but identified neither a date nor specific plotters. Commanders subsequently increased protective security at British bases.[11] This accords with author interviews: Officials acknowledged a general awareness of Iranian intent to attack European locations, building in the weeks ahead of the RAF Fairford incident.[12]

The warning arrived against the background of an active Iranian campaign. Since March 2026, arson attacks and other incidents across European cities had been claimed under the name Harakat Ashab al-Yamin al-Islamiya (HAYI), also known as the Islamic Movement of Companions of the Right (IMCR).[13] HAYI was revealed to be a façade-brand, fronting IRGC- and KH-linked individuals running a network of local criminal proxies;[e] attacks halted after one of the operatives behind the campaign, Mohammad Baqer al-Saadi, was arrested in Turkey and extradited to the United States in April.[14] By July, the British government assessed that IRGC Quds Force (IRGC-QF) members almost certainly directed HAYI's attacks.[f]

Against this increasingly alarming threat picture, the recent memories of the HAYI/IMCR campaign, and the possibility of a resumption of the U.S.-Iran conflict, British and American officials were aware of the potential for further attacks, including against military facilities. Public accounts nevertheless differ over how closely authorities were following the eventual RAF Fairford

d As noted by Tom Field in "The intelligence-operative gig economy: from surveillance to sabotage," International Institute for Strategic Studies, August 17, 2026, "[a]lthough amateur proxies are often easier for authorities to identify and disrupt, they can be used at a scale that strains the finite resources of intelligence and law-enforcement agencies. Officials in Germany, the Netherlands, Poland and the UK have all commented on their recent increase in state-threats casework. There is a growing recognition in many of these public statements that European intelligence agencies will need to manage the inherent challenge of disrupting large numbers of disposable proxy actors who can be quickly replaced."

e 'Façade' groups, in the terminology of one of the authors (Smith), are online brands used to claim kinetic attacks and make threats. Smith, along with Dr. Michael Knights and Dr. Hamdi Malik, has previously explored the role of façades and their linkage to real-world armed groups and individuals. See Crispin Smith, Michael Knights, and Hamdi Malik, "Attributing the Erbil Attack: The Role of Open-Source Monitoring," Washington Institute for Near East Policy, February 24, 2021.

f Dame Angela Eagle, in "Designation of state threats," written ministerial statement HCWS218, July 13, 2026, noted that "[t]he Islamic Movement of Companions of the Right (IMCR), otherwise known as Harakat Ashab al-Yamin al-Islamiyah, have publicly claimed seven attacks at UK locations linked to Jewish and Israeli communities, and Persian-language media, including the antisemitic arson attack on four Hatzola ambulances in Golders Green on 23 March. Sitting behind IMCR were members of Iran's Islamic Revolutionary Guard Corps Qods Force, who almost certainly directed IMCR attacks across Europe."

Name	Alleged role	Status	Nationality
Mohammad Baqer Saad Dawood al-Saadi	Central organizer with IRGC and Kata'ib Hizballah connections; attack planning and HAYI propaganda. Allegedly attempted to coordinate with associates through coded prison messages before Fairford.	Federal custody in New York, awaiting trial.	Dual Iraqi–Iranian
Mohsen Mohajeri	IRGC operative; planning, procurement contacts, targeting and propaganda. Allegedly coordinated with al-Saadi and al-Hassani.	Present in Iran during the September plot.	Iranian
Mohammed Ali al-Hassani, alias "Ali"	Overseas handler of British associates; organised Fairford reconnaissance, payments, equipment procurement and van movements. Also allegedly directed earlier HAYI attacks.	Present in Iran during the September plot; formerly resident in Britain.	Iraqi. British citizen until October 2026 (citizenship revoked by U.K. Home Office).
Mustafa Mter Rassoul Alkyaui	According to ITV, and alleged criminal intermediary. His and his brother's European underworld contacts reportedly helped recruit local attackers for HAYI attacks (though no links to the RAF Fairford case have been reported).	Detained in Turkey, according to ITV's November 11 report; organized-crime connections in the Netherlands.	Not public. Links to Iran, Iraq, and the Netherlands.
Rassoul Mter Rassoul Alkyaui	According to ITV, alleged criminal intermediary working alongside his brother, Mustafa, to connect the network with local perpetrators.	Reported at large on November 11; actual whereabouts unknown.	Not public. Links to Iran, Iraq, and the Netherlands.
Mohmed Ahmad Abdulkarim	British intermediary for Ali; allegedly enlisted the men and organised funding, vans and equipment. Charged with assisting a foreign intelligence service.	UK; Westminster, London resident. Granted conditional bail on October 27.	British, confirmed by UK police
Nouman Essghir	Allegedly conducted perimeter reconnaissance for Ali on August 22; subsequently travelled with the September van group. Charged over the reconnaissance.	UK; remanded in custody on October 27.	British, confirmed by UK police

Figure 1: Named individuals associated with HAYI attacks or the RAF Fairford plot. Listed activities are allegations only.

suspects prior to the incident.[g]

Recruitment for the Incident and Suspects (August-September 2026)

A preliminary outline of the plot's recruitment can be pieced together using the various official U.K. and U.S. statements, indictments, and police reports. On October 12, Home Secretary Shabana Mahmood told the House of Commons that the plot was highly likely to have been "coordinated by a known individual based in Iran" and "almost certainly directed by Iran's IRGC."[15] The October 27 hearing then supplied a more concrete account of recruitment and tasking. Prosecutors alleged that an overseas handler known as "Ali," believed to be acting in Iran's interests, worked through Mohmed Ahmad Abdulkarim, a 24-year-old British national living in Westminster, London. Abdulkarim allegedly recruited participants, purchased equipment, and received multiple payments from Ali totaling approximately £70,000.[16]

November's Department of Justice indictment, however, provides the most significant insight into IRGC proxy operations since the HAYI campaign and arrest of al-Saadi in April. Confirming the direct link between the RAF Fairford planners and the team behind HAYI, the indictment revealed that "Ali" is Mohammad Ali al-Hassani, an Iraqi national who previously lived in the United Kingdom[17] and provided tactical direction to the proxies behind HAYI.[18] [h] According to *The Times of London*, al-Hassani was born in Iraq in 1991 and moved to London when he was three.[19] A British citizen, al-Hassani fled to the Middle East and was stripped of his citizenship in October 2026.[20] Among various HAYI attacks, prosecutors have suggested that al-Hassani may have been connected to an incident[21] involving a quadcoptor flown at the Israeli embassy in London, which online propaganda claimed released a chemical attack (though police found non-hazardous items and said the embassy had not been attacked).

The U.S. indictment also identified Mohsen Mohajeri, an Iranian national who with al-Saadi helped plan and direct the HAYI attacks.[i] Mohajeri has been a member of the IRGC since 2004 and has claimed to have worked with the IRGC head of special operations.[22] Meanwhile, U.S. prosecutors claim that al-Saadi himself was able to coordinate with—and possibly supply funding to—al-Hassani and

g On the one hand, President Donald Trump claimed they had been "under view for a long time." See "Security increased at US Fairford air base in England," Reuters, September 27, 2026. On the other hand, some Whitehall sources claim the arrests were "not intelligence led." See Niva Yadav, "Who are the five UK nationals arrested on suspicion of 'terror' plot at RAF Fairford?" *London Standard*, September 28, 2026.

h Al-Hassani directed attacks in London by video call, in at least one case telling a proxy when and where to light and throw devices in real-time.

i In the view of the authors, Mohajeri is likely the senior member of the operation; this is based on analysis of the nature of alleged communications between al-Saadi and Mohajeri laid out in the indictment, as well as Mohajeri's age and years of IRGC service. Nevertheless, al-Saadi occupied a rarified place in IRGC and wider "Axis of Resistance" circles, as laid out by Crispin Smith and Michael Knights in "Mohammad Baqer al-Saadi: Profiling an IRGC and Iraqi Militia Operative," *CTC Sentinel* 19:5 (2026).

Mohajeri from federal prison in the days before the RAF Fairford incident, using coded messages passed via family members.[23]

Put together then, preliminary details suggest that al-Hassani drew on personal networks developed during his time living as a British citizen in the United Kingdom. During that time, al-Hassani appears to have met Abdulkarim,[24][j] and while based in Iraq or Iran, al-Hassani appears to have used Abdulkarim to recruit, finance, and supply the plot against RAF Fairford,[25] as will be detailed below.

At the time of publication, at least 11 individuals have been arrested or charged in connection with the RAF Fairford case. This includes al-Hassani, al-Saadi, and Mohajeri (all charged by the United States). In addition, five men were arrested at Whelford on September 27,[26] while a 25-year-old dual British-Iranian national and a 22-year-old British national were arrested on October 1 and 6, respectively, all initially on suspicion of preparing terrorist acts under Section 5 of the Terrorism Act 2006.[27] These seven men were initially bailed, but on October 20, police rearrested the dual national and one of the original five, 24-year-old Nouman Essghir, on suspicion of assisting a foreign intelligence service.[28]

On October 27, Essghir was charged under Section 4(1) of the National Security Act 2023 in relation to alleged activity near RAF Fairford on August 22. Prosecutors alleged that he filmed the perimeter at Ali's request. Abdulkarim, who had initially been interviewed under caution, was also charged under Section 3(2) of the National Security Act with assisting a foreign intelligence service, alleged to be Iran's, between August 31 and September 28.[29] The dual British-Iranian national was released without charge in relation to the October rearrest,[30] but remains on bail following his original arrest.

Police have said that five other men remain on bail. Abdulkarim, who is wheelchair-bound, was granted conditional bail; Essghir was remanded in custody. Both defendants are due at the Old Bailey on November 20.[31]

Preparations and Reconnaissance for the Incident (August-September 2026)

Preparations for the incident date back to at least August: U.S. prosecutors allege that al-Hassani "directed and paid associates in the United Kingdom to conduct preparatory steps and arrange logistics for the RAF Fairford Terrorist Plot." Al-Hassani is alleged to have paid an individual to perform "pre-operational surveillance" of RAF Fairford's perimeter.[32] U.K. prosecutors, meanwhile, claim that Essghir traveled to RAF Fairford to carry out reconnaissance of the base and its perimeter. Among the offenses he is accused of committing, Essghir is charged with inspecting or approaching a "prohibited place" for reasons "prejudicial to the safety or interests of the United Kingdom."[33]

Then in September, al-Hassani "tasked and paid" several individuals to prepare the plot. According to U.S. prosecutors, those individuals obtained vans and barrels of fuel. They also researched buying "chemical accelerants, including large quantities of potassium chloride, and buying metallic objects that could be used as explosive shrapnel."[34]

At least one van bore apparent fuel-delivery branding: "FUEL 2YOU" in red lettering and a telephone number. A real British fuel-delivery company, "Fuel2U," denied any connection and said its name had been used without permission.[35] Another van bore the decal of a swimming pool supply company. The likely fake livery provided a commercial cover story for vans carrying fuel near farms, and was reportedly created due to al-Hassani's urging.[36] The vans were then fitted with dashcams through which al-Hassani tracked the five men on their journey toward RAF Fairford.[37]

These allegations point toward al-Hassani believing his network was assembling a viable and potentially lethal incendiary explosive. Despite this, it appears that the local proxies did not ultimately assemble a viable device: British prosecutors allege that £300 worth of petrol (probably equivalent to around 45 U.S. liquid gallons) was put into drums in the vans before they traveled to Fairford.[38]

At the Scene of the Incident (September 26-September 27, 2026)

On the day of the planned incident, al-Hassani ("Ali") allegedly closely coordinated the movements of the five men and the three vans, directing them where to drive and providing real-time guidance on routes.[39] Upon reaching RAF Fairford, U.K. prosecutors claim that he told the men via phone call to park the vans and walk away, then informed them that their vehicles contained a bomb.[40] One of the men then called the police.[41] At approximately 00:45 U.K. time on September 27, Gloucestershire Police received the call about three suspicious vehicles apparently traveling toward RAF Fairford. Separately, a farmer returning from a party encountered the vans blocking the road near her property. She called police at 01:36 and said armed officers arrived roughly 10-15 minutes later.[42] Responding to the first call, armed officers arrested five men (including Essghir) in Whelford, just outside the base. The initial phone call to police raises the likelihood that some recruits were initially unaware of the possible terrorist purpose, but leaves an open question as to whether the organizers in Iran believed that one or more assembled bombs *had* been placed inside the vehicles.

Police took the bomb threat seriously, and established a 400-meter cordon, brought in an Army explosive-ordnance-disposal team, and evacuated 85 households.[43] On September 29, police confirmed that vehicle examinations had found petrol but no improvised explosive devices.[44][k]

U.K. National Security Charges and Updated Federal Terrorism Charges (October-November 2026)

The re-arrests on October 20 by U.K. authorities confirmed a shift toward investigating assistance to Iranian intelligence services under Section 3 of the U.K. National Security Act 2023: Police explicitly stated that "the country to which the investigation relates is Iran."[45] Under Section 3, it is an offense for a person to engage in any conduct while intending "that conduct to materially assist a foreign intelligence service in carrying out UK-related activities,"[46] or to knowingly engage "in conduct that is likely to materially assist a foreign intelligence service in carrying out UK-related activities."[47][l] In charging Abdulkarim and Essghir, U.K. police had therefore

j In Westminster Court, it was claimed that Abdulkarim had known "Ali" for 10 years.

k Court reporting on October 27 described a metal oil drum in each van, two containing petrol, alongside hard plastic water butts and internet-enabled dashcams.

l The offense occurs if the person knows or should reasonably have known that the conduct "is likely to materially assist a foreign intelligence service in carrying out UK-related activities."

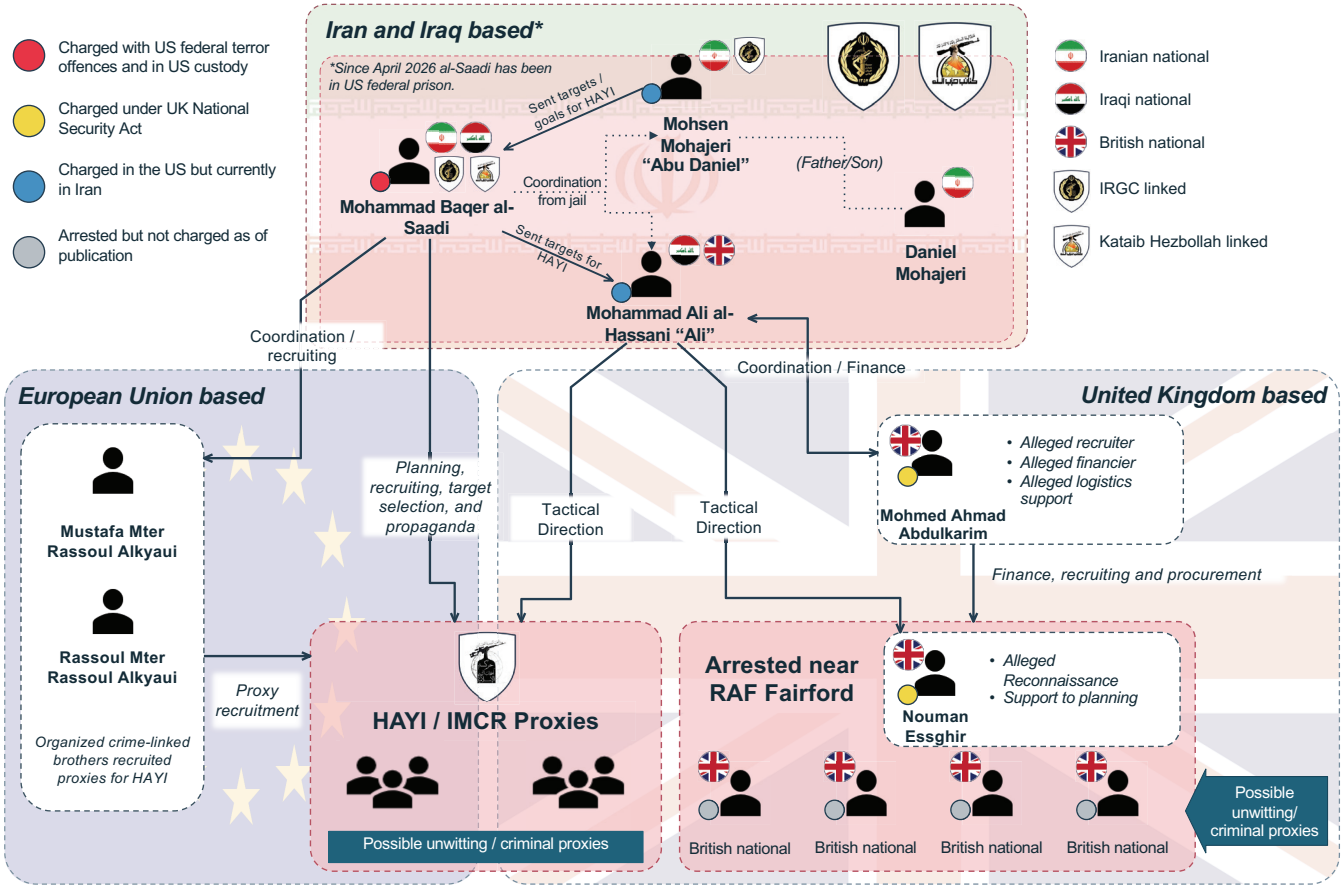


Figure 2: Preliminary organization chart based on currently available public information. Links and roles are allegations only.

developed reasonable grounds to suspect that they knew (or should reasonably have known) that their activities meaningfully assisted one or more Iranian intelligence services.

Meanwhile, the updated U.S. federal terrorism charges, unsealed on November 10, shed greater light on the IRGC operators and affiliates behind the RAF Fairford plot, while explicitly linking them to the attacks claimed by HAYI.

Incident Aftermath and U.S. Bomber Redeployment (October-November 2026)

The U.S. Air Force subsequently removed its deployed bombers from Fairford; a Pentagon official confirmed their return to home stations on October 4. On October 6, U.S. officials told Reuters that an Iranian drone threat prompted the move, without explicitly linking that threat to the September arrests.[48] (Further withdrawals from RAF Mildenhall and RAF Lakenheath would soon follow.)

The British government's attribution also became more explicit. On October 12, Prime Minister Andy Burnham assessed Iranian coordination as highly likely and IRGC direction as almost certain. A joint foreign minister statement, including the United States and European partners, recognized the U.K. attribution and connected Fairford with the IRGC's use of covert networks and proxies.[49] Iran continues to deny involvement in the incident.[50]

The United Kingdom also summoned Iran's ambassador and sanctioned Ruhollah Bazghandi, an IRGC Intelligence Organization counterespionage official, along with Shahram Ali Reza Tamarzadeh Jakki, a Zindashti criminal-network facilitator. Though the sanctioning was explicitly tied to the incident, the Foreign Office did not formally identify either individual as having been personally involved at Fairford.[51]

Preliminary Assessments of the Incident

At its most basic, the RAF Fairford incident involves the same team of Iranian-Iraqi IRGC covert operatives that coordinated the HAYI attacks from Iraq and Iran-based operations rooms earlier in the year. Some, but likely not all, of these individuals are named in the most recent DOJ indictment.[52 m] The Iranian operators themselves likely include members of the IRGC's Intelligence Organization (IRGC-IO), with Unit 4000—a covert directorate responsible for assassination, sabotage, and targeted kinetic attacks—probably playing a key role, possibly supported by the Quds Force's Unit 11000 or elements of the Ministry of Intelligence and Security (MOIS).[53]

Just as with HAYI, Iran and Iraq-based operatives once again worked through local intermediaries to recruit, supply, and pay criminal proxies to conduct attacks on distant targets. Communication with proxies or local handlers was through mobile apps, video calls, and other remote means. The alleged al-Hassani–Abdulkarim chain falls within the older playbook: Recent ITV News reporting claims that al-Saadi made similar

m Al-Saadi's Iraq- and Iran-based operations rooms are known to have had multiple other members.

"At its most basic, the RAF Fairford incident involves the same team of Iranian-Iraqi IRGC covert operatives that coordinated the HAYI attacks from Iraq and Iran-based operations rooms earlier in the year."

use of Netherlands-linked Iranian-Iraqi brothers Mustafa Mter Rassoul Alkyaui and Rassoul Mter Rassoul Alkyaui Mohsen earlier this year.[54] Both brothers have links to organized crime and used these networks to help al-Saadi recruit for HAYI attacks.[55] Still, in some cases, some recruits may not have known their ultimate sponsors' Iranian affiliations, even if the intermediaries generally had prior relationships with the handlers (at least one individual linked to the RAF Fairford plot had known al-Hassani for several years.[56]) Meanwhile, motivations may have varied from participant to participant: In other Iranian operations, recruits have acted for money,[n] ideology (particularly anti-Israel sentiments),[o] or simply boredom and a desire for adventure.[57] [p]

Given the lack of finished explosives, several scenarios remain plausible for what the Iran-based organizers had intended at RAF Fairford:

Kinetic Attack: Explosives or Incendiary Device. The suspects were told to park their vehicles and warned of bombs onboard. No bomb was found; it remains unclear whether the organizers intended this or devices failed to be loaded or properly built. The fuel could have served as an accelerant.

Kinetic Attack: Physical Intrusion. The suspects could have intended to drive through gates or fences, or scale or cut the perimeter. In 2025, Palestine Action activists breached RAF Brize Norton and vandalized military aircraft.[58] Given the reported phone call to the suspects telling them to park the vehicles and informing them of a bomb on board, this scenario now seems unlikely.

Drone-Enabled Attack. U.S. statements linking the bomber withdrawal to a drone threat raise the possibility of commercial or modified drones intended to disrupt flights, surveil the base, or attack aircraft.[59] *The Wall Street Journal* has also reported a broader RAF Fairford threat involving plans to kill American pilots and target aircraft using drones and other measures, possibly combined with vehicle-based explosives.[60] Notably, al-Saadi had a background in drone procurement for Iranian militias[61] and a deep personal interest in the potential of commercial drones as potential weapons.[62]

Information Operation and Disruption. Compatible with the other scenarios, the principal objective may have been chaos and a demonstration that apparently safe targets could be threatened. Arguably, this was achieved despite the plot being disrupted before any physical damage could be caused.

Concerningly, Iranian coordinators are unlikely to see the outcome as an unqualified failure. Disposable recruits reached the edge of a sensitive airfield and generated strategic effects at limited cost—a potentially enticing cost-benefit analysis for IRGC planners.

Iran's Tactical Shift: Using Criminals to Hit Both Soft and Hard Targets

The RAF Fairford incident is the latest development in a well-established Iranian campaign orchestrated by the same IRGC network behind the HAYI campaign. In his October 2026 threat update, MI5 Director General Sir Ken McCallum described Iran's recruitment of criminals against opposition figures, Iranian media, British Jewish communities, and Israeli targets as "subcontracting its UK violence."[63] [q] As familiar plots against soft targets proliferated, McCallum claimed that MI5 had documented "a major shift in Iranian ambitions to come at harder targets, like military sites."[64]

One of the authors (Levitt) described the beginnings of this trend in his August 2025 *CTC Sentinel* article, outlining Tehran's "homeland option" to attack Western targets using its own operatives, criminal surrogates, established terrorist proxies, and individuals inspired to act independently.[65] This drew on a 2022 study documenting shifts toward relatively deniable dual-nationals and non-Iranian citizens conducting surveillance, assassinations, and terror in Europe and the Americas. Its assessment that an empowered IRGC would become more aggressive in protecting the revolution, conducting more assassinations, abductions, surveillance, and indiscriminate attacks abroad, has been borne out.[66] The Twelve Day War and the U.S.-Iran War of 2026 may have degraded Iranian capabilities, but it also shifted internal power decisively toward the IRGC and hardline affiliates while placing the regime in existential crisis. The result is a combination of greater incentive to impose costs in Western homelands and a security apparatus increasingly disposed to do so.

Another of the authors (Smith), meanwhile, documented the rise and fall of HAYI/IMCR—and one of its dual-national Iranian-Iraqi masterminds with close ties to Iraq-based terror groups and the IRGC-QF—in a *CTC Sentinel* study published in May 2026. HAYI

n Prosecutors alleged that Iranian asset Farhad Shakeri recruited Carlisle Rivera and Jonathon Loadholt to locate and murder an Iranian-American dissident in exchange for a promised $100,000. A DOJ announcement describes messages about payments and surveillance undertaken by the recruits. "Justice Department Announces Murder-For-Hire and Related Charges Against IRGC Asset and Two Local Operatives," U.S. Department of Justice, November 8, 2024.

o Rising antisemitic and anti-Israel sentiment since the outbreak of the Gaza war has created a larger pool of individuals who may view attacks on Jewish or Zionist targets as justified. Simone Saidmehr, "How Iran is outsourcing terror plots against Jews," Forward, June 5, 2026.

p At the sentencing for Joannes Natland, a Norweigian teenager convicted of traveling to the United Kingdom to carry out a murder-for-hire on behalf of a Swedish organized crime group tied to Iran, the judge said: "The idea of being involved in such an endeavour thrilled your immature personality." She also said his messages demonstrated excitement about the planned killing.

q McCallum also warned that 2026 saw Iran attempt to expand its "hybrid campaign," and MI5's corresponding operations led to more than 50 arrests in the United Kingdom.



A U.S. Air Force crew chief signals a B-52H Stratofortress aircraft before it taxis at RAF Fairford, England, on September 20, 2025. (Staff Sgt. Tambri Cason/U.S. Air Force)

claimed at least 18 attacks, including bombings and arson, across Europe between March and April of this year, including eight in the United Kingdom, alongside at least two planned attacks against the United States.[67] In July, the U.K. foreign secretary confirmed Iran's role, stating that "sitting behind IMCR were members of Iran's Islamic Revolutionary Guard Corps Quds Force, who almost certainly directed [the attacks]."[68] The Director General of MI5 was still more blunt: "behind this front sat members of the IRGC."[69]

Those earlier attacks, primarily against Jewish-linked civilian targets, were designed to sow fear and confusion in Europe and North America, signaling Iran's ability to impose consequences in foreign homelands for the U.S.-Israeli war while terrorizing Jewish communities.[70] In the words of one of HAYI's principal coordinators, the purpose was to "[distract] the enemy" and wage "psychological warfare" to "instill fear and terror in civilians."[71] Criminal proxies were recruited in person and online by Iranian and Iranian-affiliated militia operatives based in operations rooms in Baghdad and Tehran.[72] The Iranian operators arranged payments, target selection, and even provided real-time tactical direction via video calls.[73] These typologies closely match the RAF Fairford plot. The target selection, however, suggests an increasingly strategic target set linked to broader Iranian war aims, while the overlap of key personnel implies centralized coordination of Iranian covert actions in Europe.

The earlier HAYI campaigns also point to Iran's appreciation of small-scale plots and, even more, the utility of recruiting criminals to carry them out. Unlike previous cases in which Iran used criminal cutouts to recruit operatives, the HAYI model involved the "opportunistic recruitment of disposable local operatives," which placed still greater distance between Iran and the attacks.[74] Here, Iran appears to have taken a page out of Russia's "violence as a service" playbook.[75] After nearly 1,000 covert Russian operatives were expelled following the invasion of Ukraine, MI5 said the Kremlin was "scrambling to pay criminals to do their bidding" or "exploiting naïve volunteers" organized under the GRU Volunteer Corps.[76] This violent gig economy, referred to by authorities at Europol as "violence as a service (VaaS)," typically involves the outsourcing of violence to "criminal service providers," often young perpetrators willing to act for a fee. Eleven European countries joined forces in April 2025 to create Operation Taskforce GRIMM, focused on combating the VaaS threat in Europe.[77] Since its inception, the task force's work led to the arrest of 280 suspects and the identification of over 14,000 VaaS accounts.[78]

In line with emergent Iranian VaaS patterns, al-Saadi used social media to support the IRGC, KH, and Lebanese Hezbollah and to plan, execute, and promote European attacks.[79] In February 2026, he called for attacks to avenge the death of Ayatollah Ali Khamenei. "Kill everyone who supports America and Israel," he wrote. "Do not leave any of them remaining. Civil and military targets, as well as voices of discord, kill them everywhere."[80] Soon, the Department of Justice alleges, the HAYI attacks commenced.

The extensive use of online media and infrastructure comports

with findings of a Europol operation in May 2026 that involved 19 countries that targeted 14,200 online posts in the IRGC's "propaganda ecosystem."[81] Led by its EU Internet Referral Unit, the action targeted propaganda, recruitment, and fundraising, tracing interconnected multilingual websites and material from aligned groups, including Hezbollah, Ansar Allah, Hamas, PIJ, and HAYI.[82] Likewise, al-Saadi's use of cryptocurrency in his violence-for-hire schemes,[83] is reflected in broader IRGC activities, with the latter using crypto payments to amplify online operations, a tactic Europol assesses was intended to evade detection by banks and regulators.[84]

Prior to RAF Fairford, the attacks conducted under the HAYI 'brand' were probably the most high-profile of Iran's recent homeland terror campaigns, but nevertheless represent only the tip of the iceberg of a wider effort to put pressure on counterterrorism and police forces across Europe. In July 2025, 14 governments warned that Iranian intelligence services were increasingly collaborating with international criminal organizations against journalists, dissidents, Jewish citizens, and officials in Europe and North America.[85] MI5's director has since reported more than 50 arrests in Iran-linked operations over the past year, citing Iran's use of criminal proxies to intimidate oppositionists, Iranian media organizations, Jewish communities, and, increasingly, military sites.[86]

Criminal proxy attacks in Europe over the last 18 months (as well as attempted attacks in North America and Southeast Asia) show an alarming evolution in Iranian ambition. Earlier activities focused on intimidating or assassinating journalists and Iranian dissidents, including the 2024 attack on *Iran International* journalist Pouria Zeraati in London by three hired criminals[87] and a similar foiled attack in 2025.[88] As the Iran-Israel conflict escalated, however, attacks on Israel-linked targets increased, including the alleged plot against the Israeli embassy in London disrupted by counterterrorism raids in May 2025.[89] Attacks on Jewish community interests across Europe, including HAYI's campaign, likely reflect efforts to internationalize the conflict. Now, the RAF Fairford incident points to a further worrying trend: expanding criminal proxy warfare into attacking and surveilling military targets in the United States or allied homelands (in what military strategists might refer to as the "strategic deep"). In October 2026, U.S. officials warned that Iranian plots targeting current and former U.S. officials had reached an advanced stage, and the following month, Treasury Secretary Scott Bessent moved out of his home and into protected housing on a U.S. military base as a result of Iranian threats to kill him.[90]

The expansion from soft to harder targets was only a matter of time, given Iran's intent to increase costs for allies supporting American and Israeli military campaigns and disrupt military planning, including by forcing bombers farther from the region. As the war persisted, Iranian leaders appear to have been willing to escalate their plotting and assume greater risk—still through criminal cutouts—in terrorist operations against Western countries.

In its March 2025 threat assessment, before the Twelve Day War that June, the Office of the Director of National Intelligence warned that Iran "will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States."[91]

That assessment preceded two U.S.-Israeli wars against the regime and its nuclear and ballistic missile programs. In June 2025, NBC News reported that, as the Trump administration considered striking Natanz and Fordow, Tehran threatened to "activate sleeper-cell terror inside the United States" if the military followed through.[92] The threatened sleeper-cell campaign did not materialize—perhaps because U.S. law enforcement was on high alert—but European authorities soon exposed Iranian plots against Israeli and U.S. embassies in Sweden[93] and Jewish institutions and individuals in Germany[94]—both involving criminals[95] recruited by Iran. Already then, it appears, Iran indicated a willingness to couple a campaign of multiple attacks against soft targets with a smaller number of attacks against somewhat harder targets.

"The RAF Fairford incident points to a further worrying trend: expanding criminal proxy warfare into attacking and surveilling military targets in the United States or allied homelands (in what military strategists might refer to as the 'strategic deep')."

Nine months later, against the backdrop of the second war, an Israeli national security council official told *The Jerusalem Post* that the regime in Tehran had removed operational constraints and instructed agents to recruit widely among organized criminal groups, lone actors willing to commit violence for money, and non-Iranian Shi`a militants from places like Azerbaijan and Afghanistan. Now, the official said, "where they can act, they act."[96] Plots by Iranian agents and their terrorist or criminal proxies were soon disrupted from London to Abu Dhabi and Baku to Doha.[97] IRGC involvement has been identified in many cases: the HAYI attacks and the RAF Fairford plot linked to al-Saadi (a dual Iraqi-Iranian citizen as well as an operative of both KH and the IRGC),[98] and Mohajeri (an Iranian citizen and IRGC member linked to special operations);[99] meanwhile, a report identified IRGC Colonel Ali Asgar Bordbar Sherami as "one of the main organizers" of the series of plots in Azerbaijan.[100]

Iran's expansion of external operations toward both soft and hard targets reflects a calculus that expendable criminal proxies make plots in Europe and the United States low cost and lower risk. Even when these attacks fail or are foiled, they impose costs on Western targets, as RAF Fairford and the disrupted HAYI plots underscored. Western governments are demonstrably failing to deter such plots within their borders, partly because of tepid responses to Iranian activities. Arresting disposable perpetrators, and even high-ranking operatives like al-Saadi, is unlikely to dissuade IRGC, MOIS, or proxy-group leaders from further attacks unless Western governments significantly raise Iran's costs. Indeed, even in a U.S. prison, al-Saadi is alleged to have enabled his associates to carry out more attacks using coded messages in jailhouse telephone calls.[101]

The Growing Role of the IRGC-IO

IRGC-QF has been publicly associated with the operatives behind HAYI who are now alleged to have coordinated the RAF Fairford attacks. But the October 12 U.K. sanctions also raise the possibility of an IRGC-Intelligence Organization role. Ruhollah Bazghandi, a

senior IRGC-IO official and one of the two individuals sanctioned in that tranche, runs what U.S. law enforcement refers to as the "Bazghandi Network," a group of IRGC-IO operatives involved in "lethal targeting operations" worldwide, including U.S. murder-for-hire plots.[102] The Foreign Office did not directly identify him as involved at Fairford, but his sanctioning highlights the organization's wider role. Sanctioning Bazghandi and a member of the Zindashti network in response to the RAF Fairford plot underscores the central roles of the IRGC-IO and its criminal proxies.

This could align with trends previously identified by the authors, with the IRGC-IO displaying growing intent, ambition, and capacity for covert operations in Europe and the United States.[103] Israeli sources identify Unit 4000 of the IRGC-IO as a dedicated overseas-attack capability.[104] An August 2026 *Iran International* report alleged the branch recruited deniable local proxies in Thailand and Indonesia for unrealized attacks on shipping in Asian ports and straits.[105] Two months earlier, Israeli and Azerbaijani security forces thwarted a series of IRGC-IO plots in Azerbaijan run by Unit 4000 and targeting a pipeline, the Israeli embassy, a synagogue, and Jewish community leaders.[106] Such actions indicate an increasingly strategic and wide-ranging outlook, at least on par with IRGC-QF,[107] which runs its own global cover operations unit–Unit 11000. Operatives from Unit 11000 were tied to plots targeting the Israeli ambassador to Mexico in late 2024[108] and to violence-as-a-service plots recruiting locals to target Israelis and Jews in Greece, Australia, and Germany in 2024 and 2025.[109]

Intriguingly, some public reporting claims investigators believe that *both* the IRGC-QF and MOIS were funding the network behind the RAF Fairford plot, with neither knowing that the other was involved.[110] This may explain why the United Kingdom also elected to sanction a member of a MOIS-linked crime network. The sanctioned individual, Shahram Ali Reza Tamarzadeh Jakki, was described as a "facilitator of the Zindashti criminal network, involved in several plots against Iranian dissidents."[111] Jointly designated in 2024 by the United States and United Kingdom,[112] Iranian narcotics trafficker Naji Ibrahim Zindashti and his network have used their criminal empire for transnational repression, including murder, from the United States and United Kingdom to the UAE, Canada, and Turkey.[113] The possibility of an indirect MOIS-link to the networks at Fairford may suggest that, after devastating airstrikes targeting the IRGC-IO, including Unit 4000, the MOIS may once again play a more prominent role in such plots.[114] According to an *Iran International* report, Iranian authorities are considering merging the MOIS and IRGC-IO, citing the fact that the MOIS has been left without a permanent leader since Esmail Khatib was killed in an airstrike in March 2026.[115]

Within this wider context, the RAF Fairford incident looks less like isolated activity than the latest stage in a trend in motion for at least half a decade. Criminal proxies have proved low-cost and sufficiently successful to be worth recruiting again—and early signs suggest multiple elements of Iran's sometimes fragmented intelligence services are converging on this strategy. Internal competition, empowered hardliners, and a desire to take Iran's war into the West's strategic deep encourage ever more ambitious target selection designed to achieve tactical action for strategic effect.

Strategic Potential Revealed by the RAF Fairford Incident

Whatever Iranian planners intended at RAF Fairford, no destructive attack occurred. Yet the incident reveals the strategic *potential* of criminal proxy attacks—or their threat—as a potent tool of irregular warfare.

"Iran's expansion of external operations toward both soft and hard targets reflects a calculus that expendable criminal proxies make plots in Europe and the United States low cost and lower risk."

Strategic Impact of the Disrupted Incident

Despite policing successes that may have prevented the various suspects in the RAF Fairford case from realizing serious malign activity, the incident has created several effects Iran could interpret as strategically beneficial, including both military and propaganda 'wins.'

First, the incident—or at least the threat of a drone attack coincidental in target and approximate timing—was cited by U.S. officials as the cause of strategic bomber redeployment. This is not insignificant: By contributing to, or motivating, the United States' decision to relocate key bomber aircraft back to North American bases, Iran potentially buys longer strategic warning time for future strikes while imposing greater logistical and refueling costs on the U.S. Air Force. Moreover, flying thousands of miles from the continental United States or distant forward hubs places a premium on tanker support.[116] And even at time of publication, security concerns continue to force strategic redeployments: In November, *The Wall Street Journal* reported that an Iranian threat prompted the redeployment of tankers from another U.K. base to Germany and elsewhere. Security at other U.K. bases was also reportedly raised in a manner indicating intelligence of likely terrorist action.[117] On its face, these withdrawals have been forced only on the basis of *potential* attacks. A key lesson is that actual *successful* attacks are not necessary to achieve strategic impact.

Second, the incident demonstrates both to Iranian planners and to Western governments that local proxies could reach the perimeter of a sensitive military airfield and appear to have come close to breaching the perimeter. One concern is that such bases could be attacked with drones, as highlighted most recently by unauthorized drone activity over RAF Lakenheath three days after the U.S. indictment of al-Saadi, Mohajeri, and al-Hassani.[118] Multiple official sources suggest U.K. and U.S. officials were aware in advance of potential Iran-backed threats against the base.[119] It is impossible to determine from public reporting what details were known or what tactical policing decisions preceded the arrests, but nevertheless, Iranian operatives are likely encouraged that, despite heightened threat awareness, recruits traveled from London and assembled within a few hundred feet of the site before being apprehended. The implication is that criminal proxies are difficult for authorities to monitor and deny freedom of movement.

To be sure, Iranian planners see the benefits, and Western law enforcement officials the detection challenges, of employing individuals to carry out violence as a service. Much like homegrown violent extremists, often lone offenders are not on the radar of

"A key lesson is that actual *successful* attacks are not necessary to achieve strategic impact."

law enforcement, and operatives hired in an online violent gig economy are hard to spot in advance. Iranian operatives and their proxies use social media and messaging apps to reach recruits, often young people drawn in through coded language, memes, and gamified tasks.[120] Like other homegrown violent extremists and lone offenders, in many cases the criminals hired by Iran lacked the training and sophistication of members of organized criminal or terrorist groups.

But despite this, cheap proxies can still create financial costs for domestic security budgets, particularly if used frequently. In 2024, police costs *alone* for drone incursions at RAF Lakenheath, RAF Mildenhall, and RAF Feltwell (including unattributed or Russia-linked incursions) were over £600,000. Commenting in the House of Commons on this statistic, one British parliamentarian summed up the situation: "We know that hostile states such as Russia and Iran will try to probe such bases, because it is cheap for them but potentially costly for us."[121]

Third, the incident has generated public Anglo-American friction over the suspects' handling and the security of U.K. military installations,[122] while sharpening some local residents' concerns about the security risks of hosting U.S. operations.[123] Campaigners already opposed to American bases have also seized on it to reinforce their existing objections to U.S. presence.[124] And the incident (combined with subsequent revelations of similar plots and security threats) have had the effect of creating a growing sense of vulnerability among members of the public and between allies. This is almost certainly then further exploited by Iranian information operations and propaganda.[r]

Greater Strategic Risk from Future Attacks

At the time of writing, the U.S.-Iran conflict has maintained a low, though volatile, tempo compared with the regional war of February-April 2026. Should the conflict re-escalate, it is entirely plausible that the IRGC will again pressure the United States and allies through horizontal escalation and offset actions outside the primary theater, just as they did in March and April.[s] RAF Fairford points to Iranian interest in directing proxy terror networks against hardened military targets. Lessons from the Ukraine conflict—where explosives-laden, first-person-view quadcopters launched from close range to attack strategic bombers at airbases deep inside Russian territory[125]—point to the strategic potential of criminal proxies as agents able to move freely and deploy low-cost weapons at comparatively close range during a military flare-up.

Terrorist Proxies: A Deterrent Threat

The threat of Iran-backed terrorist proxy attacks in Europe may also represent a deterrent tool for the Islamic Republic to exploit against European nations. Just the possibility of homeland escalation may deter decisionmakers in some countries from supporting—or appearing to support—the United States, or from imposing sanctions or diplomatic measures against Iran's regime. For years, fear of Hezbollah reprisals in Europe or against Europeans abroad has been a recurrent talking point in European capitals' responses to U.S. pressure to designate Hezbollah writ large as a terrorist organization, rather than just its military wing.[126] As Iran-linked plots proliferate, this is only likely to increase.

Response Considerations

Renewed conflict and increasingly ambitious IRGC-IO and IRGC-QF operations risk major strategic repercussions and greater casualties than more modest past efforts. As a result, it is important that Western governments develop genuine deterrence and effective countermeasures.

A law enforcement response to criminal proxies remains an important goal-line defense. British, European, and American services are working to counter attacks on their respective homelands. But subjects of interest may lack a recognizable ideological profile or appear involved in lesser crime, stretching finite monitoring resources. Arresting replaceable recruits is unlikely by itself to deter their sponsors. The alleged payments and role of Iran-linked intermediaries in the RAF Fairford incident underline the importance of tracing finance and communications upstream. Alongside that investigative work, it is vital to raise costs on Iran and its intelligence services.

Deterring the Iranian state through robust regulatory and diplomatic measures

The United States has extensively sanctioned Iran and its security services. In 2026, the United Kingdom and European Union imposed somewhat less comprehensive sanctions on the IRGC, with the United Kingdom explicitly linking some designations to HAYI and RAF Fairford.[127] Nevertheless, attacks should be met with measures designed to cause immediate financial pain to the IRGC. This should include measures to shut down IRGC-linked businesses and financial networks in Europe, and freezing Europe-based assets or properties of regime members and their families. The United Kingdom has yet to designate the MOIS in its entirety under either its terrorism or state-backed threat authorities.

More comprehensive sanctions can also act as a deterrent signal: In February 2026, the European Union designated the IRGC as a terrorist organization,[128] but in the view of the authors, European countries can and should go further in response to attacks, sharing intelligence to drive national-level designations of the IRGC on the European continent and to add broader lists of individuals and entities tied to the IRGC to their national and the E.U. designation lists.

Diplomatic measures, up to and including expulsions of diplomats or even the shuttering of embassies, should also be considered proportionate for clear violations of sovereignty (as

r In the November 12, 2026, House of Commons debate, one lawmaker noted that "[t]he Iranians are gaming the ludicrous image in the MAGA mind in the United States that somehow the United Kingdom is now a basket case when it comes to security and playing on the weakness of America's commitment to our security." Parliamentary Debate on United Kingdom Military Installations, November 12, 2026.

s In addition to the HAYI campaign, Iran also used its regional proxies such as Iranian-aligned militia groups in Iraq to expand the conflict with a view to putting military, economic, and diplomatic pressure on the United States and allies from multiple vectors. Michael Knights, Alex Almeida, and Crispin Smith, "Standing With Iran: The Integrated Combat Performance of Iraqi Militias During Operation Epic Fury," *CTC Sentinel* 19:6 (2026).

happened with Russian diplomats following assassination attempts in the United Kingdom and European countries), creating bright-line diplomatic consequences for any attempt to horizontally escalate the U.S.-Iran war into British and European homelands. And Western countries should also aggressively and proactively employ visa restriction authorities to deny persons involved in Iranian foreign operations, or their family members, entry into their countries.[129]

Deterring Iranian intelligence services through lawful kinetic targeting

Assassinations, arson, or terrorist attacks against Western targets conducted by criminal proxies but planned and directed by IRGC officials are almost certainly characterizable as Iranian armed attacks under international law.[130] This means attacked states may lawfully use armed force in self-defense and to prevent imminent attacks.[131]

Attacked states should generally counter criminal proxies through police and intelligence work, investigations, and lawful arrests—on their own territory or through extradition, as in al-Saadi's case. However, Iran-based handlers are unlikely to travel where they might be arrested. (Al-Saadi was only apprehended when traveling through Turkey and was reportedly surprised that Turkish authorities were aware of his activities;[132] al-Hassani fled the United Kingdom for Iraq once HAYI attacks were underway). In the view of the authors, Western governments should therefore consider targeted military force against overseas handlers to disrupt and deter attacks. This is more likely to disrupt the networks than financial sanctions alone.

Deterring would-be proxies through effective information campaigns and robust enforcement

Counterterrorism and national security laws include robust penalties for terrorism or aiding hostile intelligence agencies. Some potential criminal proxies may nevertheless be unaware that they are acting for a foreign power, may not initially realize their actions will amount to terrorism, or may underestimate the penalties ascribed to the actions they are being paid or coerced to do. To help manage this issue, governments should consider investing in information campaigns warning potential recruits of the serious consequences of violence for hire on behalf of foreign powers.

Continued focus on the role of Iranian militia proxies conducting external operations

When the criminal proxies are themselves being handled by un-proscribed militia proxies (with additional cut outs in-between), the already-difficult task of spotting and apprehending threats is complicated further.

As with the HAYI campaign earlier in the year, a nexus emerges between the IRGC, its Middle East-based militia proxies, and their external operations in the West.[133] Though closely affiliated with the IRGC, al-Saadi was also a commander in Iraq's KH militia, a U.S. foreign terror organization (but not designated in European countries).[134] The recent DOJ releases show al-Saadi requesting Mohajeri (of the IRGC) authorize conducting joint operations with KH.[135] Al-Saadi also used his links to KH to obtain Iraqi government passports, which he used (along with civilian Iraqi passports) to travel widely in Europe,[136] becoming acquainted with organized criminals and other individuals that he later drew on to recruit for his attacks.[137] At some point, al-Saadi added Al-Hassani—an Iraqi and British citizen who previously ran a security firm in London—to his network of contacts. Using his status as a British citizen, al-Hassani was also able to operate comfortably in Europe prior to the HAYI attacks.[138] This access allowed him to recruit other local nationals, allegedly including Abdulkarim who would go on to recruit for the RAF Fairford plot.

"The lessons of RAF Fairford for a potential aggressor are clear: Potential attacks are cheap, can take many forms, and need not succeed completely to have outsized strategic impact."

This raises several important considerations. First, it remains an open question to what extent Iraq-linked proxies drove the 2026 plots in Europe. With many of these groups not proscribed, opportunities abound for militiamen to slip through the cracks of immigration and visa systems. Worse, it has long been known that many Iran-backed proxy militias are deeply embedded in their host nations' governments. That was true here, where al-Saadi was able to smooth his travels using official passports and Iraqi government connections.

Comprehensively proscribing Iran-backed Iraqi militia groups, while holding third countries diplomatically and legally responsible for hosting attack cells and failing to apprehend them would go some way to closing off this particular threat vector.

Conclusion

The RAF Fairford incident and the HAYI campaign before it should serve as an urgent alert for national security officials across Europe. Like Russia, Iran is rapidly developing a criminal-proxy playbook and is likely to continue targeting civilians (including Iranian diaspora, journalists, U.S. government officials, and Jewish groups) and strategic targets (including critical national infrastructure and military bases). The lessons of RAF Fairford for a potential aggressor are clear: Potential attacks are cheap, can take many forms, and need not succeed completely to have outsized strategic impact.

Goal-line defense is not enough for this threat that blends the resources and vision of a hostile state with the low profile and unpredictability of lone actors or home-grown terror cells. Deterrence, then, is vital and must be more than symbolic; real costs must be threatened and (when necessary) imposed to prevent the worst. CTC

Citations

1 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*; "Three Iranian-Backed Operatives Indicted For Their Roles In Nearly 20 Terrorist Attacks And Attempted Attacks Across Europe And The United States," U.S. Department of Justice, November 10, 2026.
2 "CPS announces two men charged with National Security Act offences following RAF Fairford incident," Crown Prosecution Service, October 27, 2026. See also Footnote C as well as Margaret Davis, "Iran-linked incident at RAF Fairford 'not unique', spy chief says," Press Association, published by *The Irish News*, October 13, 2026. See also "Joint Statement on Iran, 12 October," Foreign, Commonwealth & Development Office, October 12, 2026, recognizing the United Kingdom's attribution of Iran's involvement in the incident at RAF Fairford on September 27, and noting the United Kingdom's conclusion that the "event demonstrates the IRGC's continued willingness to project hostile activity beyond its borders through covert networks and proxy actors."
3 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
4 Crispin Smith and Michael Knights, "Mohammad Baqer al-Saadi: Profiling an IRGC and Iraqi Militia Operative," *CTC Sentinel* 19:5 (2026).
5 "Three Iranian-Backed Operatives Indicted For Their Roles In Nearly 20 Terrorist Attacks And Attempted Attacks Across Europe And The United States," U.S. Department of Justice, November 10, 2026.
6 Ardavan M. Khoshnood, "The Islamic Republic of Iran's use of criminal intermediaries for extraterritorial assassinations and covert violence: a gray zone strategy of outsourced repression," *Small Wars & Insurgencies* 36:8 (2025): pp. 1433–1461. See also Matthew Levitt, "Tehran's Homeland Option: Terror Pathways for Iran to Strike in the United States," *CTC Sentinel* 18:8 (2025).
7 "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran,'" ITV News / PA, October 27, 2026.
8 "US removes B-1 bombers from UK base amid security concerns," Reuters, October 4, 2026.
9 "America's bomber withdrawal points to wider UK-US friction," Politico, October 5, 2026.
10 Michael D. Shear, Eric Schmitt, Megan Specia, and Adam Goldman, "Behind the mystery that first set off fears of Iranian threats at a UK military base," *New York Times*, *Irish Times* reprint, October 5, 2026.
11 Ibid.
12 Author interviews (Smith), September 2026; author interviews (Levitt), September and October 2026.
13 Smith and Knights, "Mohammad Baqer al-Saadi."
14 Ibid.
15 Shabana Mahmood, "National Security," House of Commons debate, Hansard, October 12, 2026.
16 "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
17 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
18 Ibid.
19 Mario Ledwith and Fiona Hamilton, "RAF Fairford 'mastermind' is British-Iraqi who was stripped of citizenship last month," *Times*, November 13, 2026.
20 Ibid.
21 "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
22 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26*.
23 Ibid.
24 Helena Horton, "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran,'" *Guardian*, October 27, 2026.
25 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26*.
26 "Update on RAF Fairford investigation – 12:30 28 September 2026," Counter Terrorism Policing, September 28, 2026, October 1–8, 2026 investigation updates and corrections.
27 Ibid.
28 "Two men re-arrested in the RAF Fairford investigation," Counter Terrorism Policing, October 20, 2026, within the investigation update.
29 "CPS announces two men charged," Crown Prosecution Service, October 27, 2026; "Two men charged under the National Security Act in RAF Fairford investigation," Counter Terrorism Policing, October 27, 2026; "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
30 "US Charges Three Men Allegedly Linked to RAF Fairford Incident," Great Driffield Radio, November 11, 2026.
31 "Two men charged," Counter Terrorism Policing, October 27, 2026; "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
32 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
33 Megan Sepcia, "U.K. Air Base Incident Was Coordinated by Man Acting for Iran, Prosecutors Say," *New York Times*, October 27, 2026.
34 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
35 "RAF Fairford latest: No explosives found in major incident, police say - but 'quantity of petrol' recovered," Sky News, updated September 30, 2026; "Update on RAF Fairford investigation," CTP, September 29, 2026, September 28-29 updates.
36 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
37 Sepcia.
38 "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
39 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
40 "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
41 "Two men charged under the National Security Act in RAF Fairford investigation," October 1-8 updates; "How did the RAF Fairford incident go from 'suspected bomb plot' to police bail?" Daniel Sandford and Tara Mewawalla, BBC, September 29-30, 2026.
42 "Farmer who called 999 over suspected RAF terror plot says more suspects could be at large," ITV News, September 28, 2026. See also "RAF Fairford terror suspect 'called police before local farmer', according to reports," ITV News, September 30, 2026.
43 "Two men charged under the National Security Act in RAF Fairford investigation," October 1-8 updates; "Thank you to local community following arrests in Whelford," Gloucestershire Constabulary, September 28, 2026.
44 "Update on RAF Fairford investigation – 18:00 29 September 2026," Counter Terrorism Policing, September 28, 2026, updated September 29, 2026; "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran.'"
45 "Two men re-arrested in the RAF Fairford investigation – 20 October 2026," within "Warrant of further detention granted for two men re-arrested in RAF Fairford investigation."
46 UK National Security Act (2023), Section 3.
47 Ibid.
48 "'Reported threat of possible Iranian drone attack' led US to remove bombers from RAF Fairford," Sky News, October 6, 2026; Phil Stewart, "Iran drone plot fears led US to remove bombers from UK base, US officials say," Reuters, October 6, 2026.
49 "Parliamentary Debates (Hansard)," House of Commons, Official Report, October 12, 2026, pp. 20 and 38; "Joint Statement on Iran," Foreign, Commonwealth and Development Office, October 12, 2026.
50 "2 men charged with UK national security offenses over incident at US-run military base in England," Associated Press, October 27, 2026.
51 "Foreign Secretary's statement on Iran," Foreign, Commonwealth & Development Office, October 12, 2026.
52 Author interviews (Smith), March and April 2026.
53 See, for example, Smith and Knights, "Mohammed Baqer al-Saadi."
54 Rohit Kachroo, "Seven men behind alleged Iranian terror network 'unmasked,'" ITV News, November 11, 2026.
55 Ibid.
56 Stanley Murphy-Johns, "RAF Fairford 'plot co-ordinated by handler working on behalf of Iran,'" *Standard*, October 27, 2026.
57 "Teenage hitman from Norway locked up for plotting UK murder for Iran-backed gang," ITV News Calendar, October 16, 2026.
58 Dan Sabbagh, "Pro-Palestine protesters break into RAF base on scooters and deface two aircraft," *Guardian*, June 20, 2025.
59 Eric Schmitt and Julian E. Barnes, "Potential Iranian Drone Attack Led to Exit of U.S. Aircraft From British Air Base," *New York Times*, October 5, 2026.
60 Shelby Holliday, Benoit Faucon, and Max Colchester, "Threat of Iranian Drone Attack Prompted U.S. to Pull Bombers From U.K. Base," *Wall Street Journal*, October 5, 2026.
61 Smith and Knights, "Mohammed Baqer al-Saadi."
62 Author interviews (Smith), individuals with direct knowledge of al-Saadi's past activities, April 2022 and April 2026.
63 "MI5 Director General Delivers Annual Threat Update," MI5 Security Service, October 13, 2026.
64 Ibid.
65 Matthew Levitt, "Tehran's Homeland Option: Terror Pathways for Iran to Strike in the United States," *CTC Sentinel* 18:8 (2025).

66 Matthew Levitt, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots," *CTC Sentinel* 15:2 (2022).
67 Smith and Knights, "Mohammed Baqer al-Saadi."
68 "UK sanctions Iran-linked criminal group that publicly claimed responsibility for recent attacks on Jewish locations," Foreign, Commonwealth & Development Office, July 13, 2026.
69 "MI5 Director General Delivers Annual Threat Update."
70 Smith and Knights, "Mohammed Baqer al-Saadi."
71 Ibid.
72 Ibid.
73 Ibid.
74 Adrian Shtuni, "Deniable, Disposable, Disruptive: Iran's Hybrid Warfare in Europe Demands a Proactive Response," Washington Institute for Near East Policy, May 4, 2026.
75 Lennart Pfahler and Artur Weigandt, "Disposable: The ordinary people doing Russia's dirty work," Politico, November 9, 2026.
76 "MI5 Director General Delivers Annual Threat Update."
77 "Operational Taskforce GRIMM – Tackling violence-as-a-service and the recruitment of young perpetrators into serious and organised crime," Europol, n.d.
78 "OTF GRIMM one-year anniversary: violence-as-a-service targets published on EU Most Wanted," Europol, April 29, 2026.
79 "Dual Iranian-Iraqi National Indicted for Providing Material Support to Terrorist Organizations."
80 "Iraqi National Arrested and Charged with Providing Material Support to Iranian-Backed Terrorist Organizations and Directing Attacks Targeting U.S. Citizens and Interests," U.S. Department of Justice, May 15, 2026.
81 "EU targets Iran's Revolutionary Guard propaganda ecosystem in an online crackdown," Europol, May 18, 2026.
82 Ibid.
83 *United States v. Mohammad Baqer Saad Dawood Al-Saadi*, criminal complaint, No. 26 MAG 1622, U.S. District Court for the Southern District of New York (2026).
84 "EU targets Iran's Revolutionary Guard propaganda ecosystem in an online crackdown."
85 "Statement on state threats from Iranian intelligence services: 31 July 2025," Foreign, Commonwealth & Development Office, July 31, 2025.
86 "MI5 Director General Delivers Annual Threat Update."
87 "UPDATED: Two sentenced over targeted knife attack on Iran International journalist," Crown Prosecution Service, July 3, 2026.
88 "Iran plot suspect says he discussed journalists at London embassy," Iran International, October 21, 2026.
89 Dan Sabbagh and Vikram Dodd, "Iranians arrested in counter-terrorism raids allegedly targeted Israeli embassy," *Guardian*, May 7, 2025.
90 Maggie Haberman and Jonathan Swan, "Bessent is Moved from DC-Area Home to Military Base Amid Iranian Threats," *New York Times*, November 10, 2028.
91 "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, March 2025, p. 23.
92 "U.S. claims strikes caused 'severe damage' and warns Iran against retaliation," NBC News, June 22, 2025.
93 "Security Alert – U.S. Embassy Stockholm (June 23, 2025)," U.S. Embassy in Sweden, June 23, 2025.
94 Amichai Stein, "Iran unleashing unprecedented terror campaign against Israelis abroad, senior official warns," *Jerusalem Post*, March 8, 2026.
95 "OTF GRIMM one-year anniversary."
96 Amichai Stein, "Iran unleashing unprecedented terror campaign against Israelis abroad, senior official warns," *Jerusalem Post*, March 8, 2026.
97 Yaron Avraham, "[Exclusive: Iran tried to harm Israeli diplomats in the United Arab Emirates]," N12, March 3, 2026; "State Security Announces Apprehension of Two Cells Linked to Iranian Revolutionary Guard," Qatar News Agency, March 3, 2026; Lizzie Dearden, "2 Charged With Surveillance for Iran on London's Jews," *New York Times*, March 18, 2026; Nadira Tudor, "Azerbaijan releases footage after foiling Iran-linked plot targeting pipeline and Jewish sites," Euronews, March 7, 2026.
98 "Dual Iranian-Iraqi National Indicted for Providing Material Support to Terrorist Organizations."
99 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*.
100 Tudor.
101 "Iranian 'terror mastermind' feared to be plotting attacks from behind bars," Maryland Coordination and Analysis Center, October 21, 2026.
102 "Foreign Secretary statement on Iran, 12 October," Foreign, Commonwealth & Development Office, October 12, 2026; "U.S. Attorney Announces Murder-For-Hire Charges Against IRGC Brigadier General And Former Intelligence Officer And Members Of An Iranian Intelligence Network," U.S. Attorney's Office, Southern District of New York, October 22, 2024; "Treasury Sanctions Officials of Iranian Intelligence Agency Responsible for Detention of U.S. Nationals in Iran," U.S. Department of the Treasury, April 27, 2023.
103 Levitt, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots." See also "Iran," Intelligence and Security Committee of Parliament, July 10, 2025.
104 "[Shin Bet and IDF thwarted the smuggling of advanced Iranian-origin weapons destined for Judea and Samaria]," Israel Security Agency, March 25, 2024.
105 Mojtaba Pourmohsen, "IRGC Unit 4000 plans attacks on shipping in East Asia, sources say," *Iran International*, August 31, 2026.
106 "Mossad, IDF and ISA Joint Announcement - 20 April 2026," Israeli Ministry of Foreign Affairs, April 20, 2026.
107 Ibid.; Mojtaba Pourmohsen, "IRGC Unit 4000 plans attacks on shipping in East Asia, sources say," *Iran International*, August 31, 2026.
108 "Mexico Thwarted Iranian Plot to Assassinate Israeli Ambassador, Officials Say," *Times of Israel*, November 7, 2025.
109 "Prime Minister's Office–Mossad," Israeli Prime Minister's Office, October 26, 2025.
110 Kachroo.
111 "Foreign Secretary statement on Iran, 12 October."
112 "UK and US step up action to tackle domestic threat from Iran," Foreign and Commonwealth Office, January 29, 2024.
113 "The United States and United Kingdom Target Iranian Transnational Assassinations Network," U.S. Department of the Treasury, January 29, 2024.
114 Matthew Levitt, "Between Intent and Capability: Assessing the Lack of Iranian Attacks on the U.S. Homeland," War on the Rocks, May 6, 2026.
115 Behrouz Turani, "Iran's Intelligence Merger Debate Signals Possible Security Shake-Up," *Iran International*, November 13, 2026.
116 "Mapping where US bombers are based globally," Al Jazeera, October 6, 2026.
117 Shelby Holliday and Alexander Ward, "U.S. Aircraft Evacuated From Second U.K. Base Due to Iran Threat," *Wall Street Journal*, November 9, 2026.
118 "Drone Activity Over US Base in Britain Prompts Security Response," Associated Press, November 14, 2026.
119 Shear, Schmitt, Specia, and Goldman.
120 "Operational Taskforce GRIMM."
121 Parliamentary Debate on United Kingdom Military Installations, November 12, 2026.
122 "America's bomber withdrawal points to wider UK-US friction."
123 Chad Garland and Devin Klecan, "Near RAF Fairford, suspected terrorism plot makes Iran war feel close," *Stars and Stripes*, October 15, 2026.
124 Ceren Sagir, "'Time to end the US's unaccountable military presence in Britain,'" *Morning Star*, October 5, 2026.
125 Kateryna Bondar, "How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare," Center for Strategic and International Studies, June 2, 2025.
126 Matthew Levitt, "Debating the Hezbollah Problem," Washington Institute for Near East Policy, January 22, 2018.
127 "Support for IRGC Outlawed in Crackdown on Foreign State Proxies," UK Government, July 13, 2026.
128 "EU terrorist list: Council designates the Islamic Revolutionary Guard Corps as a terrorist organisation," Council of the European Union, February 19, 2026.
129 See, for example, "Announcement of Additional Visa Restriction Targets for Individuals Involved in Inhibiting Iranians' Rights to Freedom of Expression," U.S. Department of State, February 18, 2026.
130 Effective control test. Level of coordination seen in HAYI cases likely arises to the threshold.
131 United Nations Charter article 51. See also, "Caroline Case," Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton, British Special Minister (Aug. 6, 1842), reprinted in John Bassett Moore, *A Digest of International Law* § 217, at 412 (1906); "Attorney General's speech at the International Institute for Strategic Studies," UK Government, January 11, 2017.
132 Author interviews (Smith), Iraqi officials familiar with the case, April 2026.
133 Smith and Knights, "Mohammed Baqer al-Saadi."
134 Ibid.
135 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*; "Three Iranian-Backed Operatives Indicted For Their Roles In Nearly 20 Terrorist Attacks And Attempted Attacks Across Europe And The United States," U.S. Department of Justice, November 10, 2026.
136 Smith and Knights, "Mohammed Baqer al-Saadi."
137 Kachroo.
138 *United States of America v. Mohammad Baqer Saad Dawood al-Saadi Superseding Indictment SI 26 Cr. 220*; Ledwith and Hamilton.