HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR NEW MIDDLE EAST

Research Brief

HOW TO PROSCRIBE THE IRGC: LEARNING COMPARATIVE LESSONS FROM OUR ALLIES

by PROFESSOR MATT QVORTRUP

JUNE 2025

Iranian Islamic Revolutionary Guard Corps troops marching in Tehran, Iran, on 4th November 2022, by saeediex at Shutterstock (https://www.shutterstock.com/image-photo/tehran-iran-november-4-2022-line-2329974559)

About the Author

Professor Matt Qvortrup is Director of Research at HJS. Also a Senior Research Fellow at the Australian National University, he is a former mediator for the United Nations, and was a member of the US State Department Envoy Team in 2009-2010.

Acknowledgements

Matt Qvortrup is grateful for research assistance by Mr Mikhail Kobelyan.

About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances that keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world. The Henry Jackson Society is a company limited by guarantee registered in England and Wales under company number 07465741 and a charity registered in England and Wales under registered charity number 1140489.

For more information, please see **www.henryjacksonsociety.org**.

About the Centre for New Middle East

The **Centre for New Middle East** is a one-stop shop designed to provide opinion-leaders and policy-makers with the fresh thinking, analytical research and policy solutions required to make geopolitical progress in one of the world's most complicated and fluid regions.

Established following the fallout from the Arab Spring, the Centre is dedicated to monitoring political, ideological, and military and security developments across the Middle East and providing informed assessments of their wide-ranging implications to key decision makers.

Contents

Executive Summary

The Islamic Revolutionary Guard Corps (IRGC) is not simply a foreign policy tool of the Iranian state – it is a prototypical *hybrid actor* that blends ideological commitment, transnational criminality, state sponsorship and covert subversion. Its presence in the UK, from academic infiltration to financial laundering and diaspora coercion, has exposed not just gaps in countermeasures – but foundational weaknesses in Britain's security architecture.

While current UK responses rely on targeted sanctions, sectoral oversight and case-by-case enforcement, this approach misreads the nature of the threat. Teheran's covert wing operates across sectors because the UK governs them in narrow corridors. It exploits outdated assumptions: that terrorism is always non-state, that financial irregularity is a regulatory not a security issue, that academic openness is only a question of ethics. This institutional myopia allows hostile networks to operate in plain sight.

This policy brief contends that the UK must reconceive its national security framework to address the strategic convergence of state and non-state capabilities. It must respond not to *Iranian aggression per se*, but to the modern shape of adversarial influence. Proscription of the entities linked to Iranian foreign branches (such as the IRGC) is necessary, but institutionally insufficient: without legal reform, inter-agency fusion and institutional recalibration, such designations remain symbolic.

We propose a security doctrine that draws on three models:

Sweden's political framing: The act of proscription as domestic protection, bound in legal, institutional and sovereign security, not international provocation

Canada's institutional integration: Institutional and parliamentary similarity between the Canadian and the British systems presents an opportunity for a streamlined and established method when combatting such adversarial hybrid actors

The United States' politico-military strategic thinking: Such proposed institutional and diplomatic shifts can be better shaped through our strategic allies' attempts at similar decisions – through their experience – shaping a more efficient institution-wide amendment would result in less political, domestic and international costs. While also providing synergistic value to international efforts at curbing threats.

Therefore, the UK must modernise its legal tools (e.g., revising the Terrorism Act 2000 and establishing a hybrid threat classification) to operationalise intelligence coordination; through a dedicated taskforce, and through such taskforce initiatives – align financial, academic and community-facing institutions under a coherent threat perception.

Without systemic recalibration, the IRGC (and actors like it) will continue to test, exploit and, as a result, outpace the UK's legacy institutions. The cost is not only strategic drift, but the erosion of sovereign resilience.

Introduction – Critical Assessment of Institutional Blind Spots in the UK

The UK's national security framework remains structurally aligned with a threat environment that no longer exists. Its primary enforcement architecture – across terrorism, financial crime, intelligence operations and civil regulation – continues to reflect post-9/11 assumptions about the nature of adversarial actors: that they are either state-driven and hierarchical or non-state and ideologically radical. Hybrid actors – entities that combine elements of both – do not fit cleanly into either model. As a result, they are often acknowledged in principle but unaddressed in policy.

This institutional misalignment is not anecdotal or episodic. It is systemic. The Islamic Revolutionary Guard Corps (IRGC) provides the clearest operational example of how hybrid actors now function within, not outside, liberal democratic legal and regulatory ecosystems. The IRGC's activity in the UK has included academic partnerships, charitable networks, community outreach and criminal facilitation – but these are not separate domains of engagement. They are coordinated operational expressions of a single actor whose structure has been explicitly designed to evade detection by systems that treat financial oversight, academic governance and ideological security as distinct arenas.

This disaggregation reflects a foundational design flaw in the UK's threat architecture. Intelligence agencies remain segmented by mandate and jurisdiction. Regulatory bodies operate independently, without a framework for national security relevance unless statutory exceptions are invoked. Legal instruments, such as the Terrorism Act 2000, define organisational threat based on demonstrable violence or direct support for terrorism – criteria which hybrid actors routinely circumvent through diffusion, legal compliance and proxy activity. As a result, adversarial entities are often visible in parts, but never classified as a whole.

What this reveals is not simply a lag in enforcement but a failure of strategic alignment. The UK retains technical sophistication across agencies – its financial regulators, domestic intelligence services and law enforcement bodies are globally respected. The gap is not in capacity but in doctrinal cohesion: there is no unified schema for understanding, designating and dismantling actors who cross institutional boundaries by design.

The consequences of this gap are not hypothetical. Hybrid actors use the space between policy domains as operational territory. They do not need to conceal activity if their activity is invisible to the architecture designed to detect it. This brief argues that, as an example, the IRGC's presence in the UK is not primarily a reflection of Iranian strategic expansion – but of British institutional design remaining anchored to obsolete threat evaluation models.

The problem is compounded by the UK's reliance on reactive legal and regulatory instruments. Enforcement thresholds are calibrated around observable violations, not around risk modelling of actor architecture. This reflects a broader issue: the UK's security response remains focused on actors' behaviour, not their structural composition. Hybrid entities exploit this distinction. They behave lawfully while building the operational capacity to act adversarially when required. The system does not trigger until the damage is already in motion.

This brief does not argue that the IRGC is exceptional. It argues that the UK's current national security infrastructure is vulnerable to any actor that shares the same operational profile:

distributed, legally embedded, ideologically coherent and tactically incremental. The IRGC simply reveals, in its most advanced form, what remains a general exposure.

The objective of this policy brief is therefore not to add another designation to the UK's sanctions list, but to introduce the feasibility of institutional, legislative and operational reforms, which would be required in order to restore strategic, sovereign control. Without a recalibrated framework – one that acknowledges the integrated nature of hybrid threats – the UK will continue to address individual incidents while leaving the structural vulnerability intact.

The Political Window Already Exists

The measures set out in this brief fall within the Government's already stated priorities. Hybrid threats were explicitly identified during the election campaign as a strategic risk to UK institutions, public safety and diaspora communities. Commitments were claimed to be made to reform national security doctrine, modernise enforcement against foreign interference and push toward a more joined-up model of institutional resilience. That language aligns directly with the actions proposed here.

This means the groundwork is already in place. The political argument has been made publicly. Parliamentary support exists. No new mandate is required – only follow-through. Proscription of the IRGC, tighter regulatory coordination and a shift toward pattern-based threat tracking are not escalatory moves. They are consistent with what this Government has already said it will do.

The advantage of timing matters. Strategic shifts face the least resistance when justification, tools and political permission align. Right now, all three are in place. That window will narrow as operational pressure builds elsewhere. This is a moment for execution, not invention.

The Anatomy of the Hybrid Actor

The IRGC functions not as an outlier, but as a case study in the evolving architecture of hybrid threats. Its operational model reflects a deliberate blending of state sponsorship, ideological cohesion, non-state flexibility and transnational access. What distinguishes the IRGC is not its existence within Iranian state structures, but its ability to operate across domains that remain legally, operationally and institutionally unconnected in most democratic systems. This cross-domain reach has not emerged by accident – it exploits design logic embedded within the UK's own national security ecosystem.

At the financial level, IRGC-affiliated entities are able to circulate capital through UK-registered charities, cultural associations and seemingly unrelated shell companies. These vehicles exist within a legal infrastructure that prioritises transactional scrutiny rather than network-based affiliation. Current financial oversight mechanisms depend on detecting anomalies within the behaviour of a given entity. However, hybrid actors do not rely on anomalous behaviour. They rely on distributed normality – spreading small transactions, diffused actors and plausible associations across multiple compliant structures. This reduces the probability of detection within any single regulatory system, particularly one where inter-agency intelligence fusion is non-compulsory and constrained by legislative thresholds.

More critically, the UK's financial monitoring system operates with a narrow definition of threat relevance. While individual transactions may flag for financial irregularity, there is no legal mandate – or risk model – that requires financial institutions to assess strategic alignment or foreign-state affiliation. This is a doctrinal lag: the assumption that hostile actors will behave outside legal norms, rather than through them. The IRGC leverages that assumption as operational cover.

In the academic domain, the IRGC has pursued access to dual-use technology and scientific expertise by forming research partnerships with UK universities through Iranian institutions that maintain formal links to Iran's security apparatus. These engagements often comply with formal institutional review processes, yet those processes operate under a legacy model that sees ethical integrity and research transparency as sufficient filters. There is no systematic protocol for assessing whether a foreign academic partner is directly subordinate to a military or paramilitary chain of command. Nor is there routine intelligence vetting of collaborative proposals unless export control laws are explicitly triggered. The IRGC exploits precisely this boundary: its partners present as academic but act in support of military-industrial priorities.

This is not simply a regulatory oversight – it is a structural assumption about the autonomy of knowledge production. British academic governance frameworks treat national security as external to research development, and this creates a doctrinal vacuum: intelligence services are positioned as reactive observers, not embedded participants in institutional risk mitigation. As a result, exposure is not just possible – it is procedural.

Community influence operations reveal a similar logic. Organisations with IRGC-aligned ideological and theological mandates have been able to establish long-term presence within UK civic and religious life. These institutions enjoy full legal protection and are engaged in community education and cultural programming. However, within these activities, there are documented patterns of diaspora surveillance, indirect coercion and identity-based political conditioning. The problem lies in classification: these are not foreign propaganda outlets in the conventional sense, nor do they fall under current radicalisation threat typologies.

Counter-extremism tools such as Prevent are structurally configured to identify *non-state religious radicalisation*, not state-sponsored ideological reinforcement. The IRGC has adapted to this distinction, embedding its influence within environments that are legally safeguarded and culturally legitimate.

What this reveals is a vulnerability not of surveillance capacity, but of institutional logic. The current system requires that threat indicators fit into predefined categories – terrorism, foreign interference, organised crime – each of which corresponds to a different agency, statute and evidentiary threshold. But hybrid actors function precisely in the space between those categories. They are neither fully state nor fully non-state; their transactions are legal until aggregated; their partnerships are benign until contextualised. This interstitial presence means that by the time an actor becomes visible, it is often already operationally embedded.

Moreover, the UK's legal architecture does not currently support network-based designations. Proscription remains focused on organisations with clear, exclusive engagement in terrorism. The IRGC, by contrast, derives strength from its ability to operate legally in some contexts and covertly in others. Its dual posture is precisely what exempts it from current mechanisms of suppression. The UK has no legislative instrument that allows for partial-state actors with blended mandates to be recognised as security threats without requiring proof of direct involvement in unlawful activity.

This exposes a deeper institutional failure: the persistence of threat compartmentalisation. Intelligence is gathered by agencies that are structurally segregated; financial intelligence, domestic extremism monitoring, foreign influence assessments and academic partnership oversight all operate along separate tracks, using distinct evidentiary standards. There is no institutional mechanism that mandates *strategic synthesis* – the act of recognising a distributed pattern of lawful activity as indicative of a hybrid security threat.

The IRGC does not merely exploit these gaps – it depends on them. It has engineered its operational presence to function within, rather than outside, the seams of liberal regulatory and legal structures. This is not a matter of the UK "falling behind" on enforcement. It is a matter of the UK operating under a legacy threat taxonomy, one that no longer corresponds to the behavioural realities of adversarial actors.

Understanding the IRGC is therefore not an exercise in regional analysis – it is an exercise in institutional reflection. If this actor can persist, embed and expand within the UK without triggering a coordinated response, the failure is not one of awareness but of strategic design.

Institutional Inadequacy – The Security Architecture Gap

The UK's existing security institutions remain shaped by legacy frameworks that are poorly adapted to the operational logic of hybrid actors. The capacity to detect, assess and disrupt these actors is distributed across multiple government bodies – each operating with distinct mandates, legal authorities and evaluative criteria. This fragmentation is not incidental. It is a structural outcome of how Britain has historically organised its response to threats: through classification, not integration.

At the legal level, the UK continues to rely on statutory definitions of terrorism and foreign interference that prioritise overt hostility, direct organisational affiliation or support for proscribed groups. The Terrorism Act 2000 remains the primary tool for organisational designation, but its applicability to hybrid entities is limited. Groups like the IRGC – formally embedded in a state structure but engaged in transnational subversion – do not fall easily within its remit. The Act presumes that proscribed groups operate outside legal and state frameworks. Hybrid actors deliberately invert this assumption by operating *within* them. As a result, UK authorities are constrained by legal instruments that were never designed to address state-affiliated actors operating through civil, financial and cultural proxies.

This legal inflexibility translates into operational constraint. MI5, the National Crime Agency (NCA), HM Treasury, the Charity Commission, the Financial Conduct Authority (FCA) and various elements of the Home Office all possess partial visibility into aspects of hybrid activity. However, their mandates are defined by separate statutes, case law and internal directives. There is no unifying operational doctrine for hybrid threat identification, nor a common classification system to facilitate threat tagging across institutional boundaries. Intelligence on IRGC-linked entities gathered by one agency may not be actionable by another, not due to classification level, but because there is no shared strategic or legal basis to define the actor as a threat.

This is not due to a failure of inter-agency cooperation – it is because of the absence of **a framework for convergence**. The current approach relies on coordination through ad hoc task forces or cross-departmental communication, which are often reactive, resource-contingent and bounded by political will. These structures are not institutionalised and therefore cannot sustain the continuous cross-sector threat-modelling required to monitor hybrid actors with embedded legal presence. Risk assessments generated in one domain – academic research, financial transactions, cultural outreach – do not automatically trigger security scrutiny unless threshold criteria are already met. In hybrid threat cases, the problem is precisely that individual activities remain below conventional thresholds until their cumulative function is already operational.

The financial domain offers a clear example. The FCA and NCA share data on illicit flows, but strategic attribution of financial networks to foreign-linked hybrid actors remains outside standard practice. Treasury sanctions frameworks are applied based on designated individuals or entities, not network affiliation. This model presumes that adversarial actors can be isolated through their direct violations. Hybrid actors, by contrast, diffuse their activity through legal structures, making enforcement a function of institutional alignment rather than detection capacity.

The academic sector faces a related, though distinct, challenge. Universities operate under the assumption that research openness and international collaboration are net strategic goods. Export control compliance is enforced, but there is no structured coordination between higher education institutions and the security services around foreign academic partnerships unless export law is explicitly triggered. Risk exposure assessments are left to local governance frameworks, which vary widely and are not designed to account for indirect state alignment. Consequently, research programmes with strategic sensitivity may proceed under full institutional transparency while remaining invisible to national security architecture.

At the operational level, the lack of a hybrid threat classification creates a vacuum in threat tracking. Law enforcement databases, financial watchlists and community safeguarding protocols are not integrated through a shared understanding of what constitutes a hybrid actor. A proxy charity flagged by the Charity Commission is not automatically cross-referenced against Treasury watchlists or MI5 alerts. Community outreach structures designed to monitor non-state radicalisation are not configured to identify state-sponsored ideological activity. This segmentation prevents the development of a longitudinal threat picture.

What results is a security system that remains technically capable but strategically misaligned. Each domain possesses its own enforcement logic. But adversarial actors do not observe those boundaries. The IRGC's operational model assumes that civil institutions – banks, universities, religious centres – are structurally unprotected from hostile but legally embedded activity. That assumption has proven largely correct. The UK's architecture is not failing in detection, but in recognition: the system cannot classify what it cannot define.

This is not a call for institutional centralisation, but for strategic synchronisation. Hybrid actors will not be addressed by more resourcing alone, nor by expanding the remit of a single agency. What is required is a new architecture of coordinated authority, where legal instruments, regulatory bodies and intelligence functions operate with shared classifications, operational triggers and escalation pathways. Without this, hybrid activity will continue to fall between institutional definitions – and strategic response will remain fragmentary by design.

Comparative Security – The Case for a Diversified Approach

The challenges posed by hybrid actors are not unique to the UK. States across the democratic spectrum are encountering variants of the same structural problem: national security frameworks that are legally robust but conceptually outdated. While the specifics of their institutional arrangements vary, Sweden, Canada and the United States have all undertaken significant reform initiatives – political, legal or institutional – in response to the operational ambiguity of actors like the IRGC.

This section does not treat these countries as models to be emulated in totality. Rather, it draws out the underlying principles of their respective adaptations: how political framing can unlock legal capacity; how parliamentary systems can integrate fragmented mandates; and how doctrine can evolve to meet actors that defy conventional categories. Each case reveals different pathways to structural realignment – and offers the UK practical options for reconfiguring its response architecture without sacrificing legal proportionality or constitutional integrity.

Sweden: Reframing Proscription as Domestic Protection

Sweden's decision to pursue the proscription of the IRGC marked a decisive shift – not in legislative capacity, but in political framing. The Swedish Government did not introduce new laws, nor did it attempt to recast terrorism definitions. Instead, it reoriented the rationale for proscription from international signalling to domestic protection. This reframing enabled the state to act within existing legal parameters by presenting the IRGC not as a foreign policy issue, but as a direct threat to Swedish civic space.

Sweden faced multiple attempted coercions, surveillance operations and transnational repression incidents tied to the IRGC. However, the significance lay in how these were narratively recast: the state argued not that Iran was hostile, but that Sweden's own communities were being infiltrated and harassed by a foreign security service. This repositioning depoliticised the designation debate and pre-empted the usual diplomatic objections – especially from foreign policy and trade constituencies – by rooting the action in the protection of sovereignty, legal integrity and democratic accountability.

The practical outcome was a political consensus that allowed the Government to request the EU to designate the IRGC under its terrorism framework while also preparing unilateral domestic actions. Swedish ministers presented the issue as a failure of state duty to protect citizens and residents from foreign ideological interference. Notably, public communication avoided inflammatory rhetoric; the IRGC was discussed not in theological or geopolitical terms, but as an *illegitimate extension of foreign law enforcement on Swedish soil*.

The lesson for the UK is clear: the political obstacle to IRGC designation is not legal capacity, but strategic narrative control. The UK has existing instruments through the Terrorism Act 2000 that allow for proscription based on threat to life or public order. What has prevented action thus far is a perception that designation is inherently provocative. Sweden demonstrates that proscription can be domesticated – rendered as an act of legal defence, not diplomatic aggression.

This reframing also allowed Sweden to bring diaspora groups into the policy process as stakeholders rather than passive beneficiaries. Iranian-Swedish civil society organisations were consulted not just on the harm posed by the IRGC, but on the political impact of inaction. This built a civic rationale that strengthened legitimacy and reduced the potential for community backlash.

For the UK, the applicability is direct: the Iranian diaspora in Britain has faced similar patterns of harassment, ideological pressure and transnational repression. Yet these incidents are still processed as isolated cases, not as evidence of systemic ideological infrastructure. Sweden's approach demonstrates how reframing the IRGC as a *domestic actor operating through foreign legitimacy* can unlock legal instruments that already exist, but that remain politically dormant.

Canada: Institutional Integration through Parliamentary Logic

Canada's approach to the IRGC reflects a different type of innovation: institutional reconfiguration without statutory overhaul. While the Canadian Government did pursue formal designation of the IRGC under anti-terror legislation, the core innovation lay in how parliamentary structures were used to legitimise and coordinate a multi-agency response.

Canada, like the UK, operates within a Westminster-derived parliamentary system, a dual-chamber legislature and a common law legal tradition. These similarities are not cosmetic. They shape how intelligence is gathered, scrutinised and operationalised. The Canadian case is particularly instructive because it shows how integration can be achieved inside an existing constitutional model.

Faced with growing evidence of IRGC-linked influence operations – spanning academic partnerships, diaspora surveillance and proxy fundraising – Canadian intelligence services were encountering the same friction as their UK counterparts: partial visibility, jurisdictional constraint and weak legal traction. Rather than create a new agency or law, the Canadian Government used existing parliamentary oversight mechanisms to coordinate mandates.

The pivotal mechanism was the integration of hybrid threat intelligence into public safety briefings. The Standing Committee on Public Safety and National Security began to receive cross-departmental reporting not only on IRGC activity, but on the structural vulnerabilities it revealed. This formalised a recognition that counter-hybrid activity required sustained inter-agency visibility – not just episodic coordination. Crucially, it also used Parliament as a convergence point, allowing ministerial alignment across Public Safety, Global Affairs, Immigration and Treasury portfolios.

Operationally, Canada created joint tasking arrangements between CSIS (intelligence), FINTRAC (financial monitoring) and the RCMP (enforcement). These arrangements were not dependent on new legislation. They were established through ministerial instruction and parliamentary mandate. This allowed for the construction of pattern-based enforcement triggers: rather than waiting for a terrorist act or explicit legal violation, these agencies could act on indicators that an actor was functionally operating as a proxy to a hostile intelligence entity.

Canada also used designation as a strategic anchor, not an end in itself. The IRGC was listed under the Immigration and Refugee Protection Act, which allowed for targeted visa restrictions and disqualification of affiliated individuals from residency. This reduced the political burden of invoking criminal or military language while achieving effective disruption.

For the UK, the implications are significant. Canada shows that structural integration of intelligence, enforcement and financial disruption tools can be achieved through parliamentary logic – without constitutional redesign. The UK Parliament has existing oversight bodies, ministerial portfolios and inter-agency mechanisms that, if re-tasked, could produce the same outcome: a pattern-based, system-wide approach to hybrid actor disruption.

Moreover, the Canadian case illustrates the value of embedding hybrid threat language into legislative and public safety discourse. By normalising this category within official documentation and ministerial communication, Canada established the basis for longer-term institutional memory. The UK, by contrast, still treats each IRGC-linked incident as a unique case. Canada's approach provides a methodology for turning a case log into a threat category.

United States: Strategic Coherence through Redundant Mechanisms

The United States offers a contrasting – but still valuable – example. Its designation of the IRGC as both a Foreign Terrorist Organization (FTO) and a Specially Designated Global Terrorist (SDGT) reflects a doctrinal willingness to apply overlapping legal regimes to a single entity. This dual-layered designation created redundancy across enforcement domains: criminal prosecution, financial interdiction, diplomatic isolation and immigration exclusion could all proceed under different authorities.

Unlike Sweden or Canada, the US operates under a national security doctrine that centralises threat classification within the executive branch. But its approach to the IRGC reveals two key insights: first, that redundant legal authority creates operational resilience; and second, that hybrid threats require horizontal engagement across agencies – State, Treasury, Homeland Security, Defense – not just vertical prosecution.

What distinguishes the US model is not its scale, but its doctrinal clarity. The IRGC is not treated as an ideological actor, nor as a religious force, but as a military-intelligence unit functioning in parallel to state diplomacy. This doctrinal clarity simplifies agency engagement: actors need not determine *whether* the IRGC qualifies as a threat – only *how* to engage with it under their existing powers.

For the UK, the direct transferability of US mechanisms is limited by legal and political structure. However, the strategic principle is fully applicable: overlapping legal instruments, if well coordinated, reduce the risk of legal inaction. A UK designation under the Terrorism Act 2000, coupled with expanded sanctions via the Sanctions and Anti-Money Laundering Act 2018, and clarified visa restrictions under immigration rules, could create a similar cumulative effect.

The US experience also illustrates how political cost can be reduced through doctrinal certainty. By embedding IRGC designations into a broader national strategy on malign influence, Washington avoided episodic political backlash – actions were framed as procedural consequences of established doctrine, not political choices requiring fresh justification.

Synthesis – Strategic Convergence and British Adaptation

Taken together, these cases demonstrate strategic convergence on the core challenge: hybrid actors require national security systems that are both integrated and adaptive. Sweden reveals the power of political reframing to activate dormant legal capacity. Canada shows how parliamentary structures can be leveraged to coordinate multi-agency response within a shared institutional logic. The United States illustrates the value of layered legal mechanisms and doctrinal clarity to sustain enforcement and reduce friction.

For the UK, each case offers a structural lesson, not a policy template. No single model is sufficient – but all three show that existing democratic systems have begun to confront the operational ambiguity of hybrid actors with concrete institutional changes. These cases validate the core premise of this brief: that the UK's current exposure to actors like the IRGC is not due to lack of will or intelligence, but due to a misalignment between institutional design and adversary structure.

What is now required is not emulation, but synthesis. The UK must build its own hybrid threat doctrine, rooted in legal proportionality, operational interoperability and political legitimacy. The elements are available. The precedent is set.

Policy Blueprint – A New UK Security Doctrine

The preceding sections have diagnosed a clear institutional vulnerability: the United Kingdom's current security architecture is not designed to recognise, track or disrupt the operational structure of hybrid actors. The IRGC, as the most mature expression of this threat category, reveals not only gaps in policy implementation but in strategic classification itself. To close this gap, the UK does not require wholesale institutional reinvention. It requires a coherent, hybrid threat doctrine, adapted to its legal culture, operational posture and parliamentary governance.

I. Reframing Threat Perception

The UK must begin by revising its conceptual categories. Current classification systems – terrorist, criminal, foreign agent – fail to encompass actors that operate legally across domains while functioning strategically as extensions of hostile intent. The IRGC is neither exclusively criminal nor exclusively state – it is a trans-sovereign actor with embedded domestic presence.

A future-ready doctrine must adopt pattern-based designation, recognising that strategic threat can emerge from the aggregation of legal activity. Sweden's security-first framing and Canada's pattern recognition mechanisms offer practical models: neither required the creation of new actor categories, but both acknowledged that existing labels were insufficient to describe the threat in front of them.

II. Establishing a Strategic Convergence – Without Structural Centralisation

Reform must begin not with the creation of new institutions, but with the alignment of existing ones under a shared operational logic. As Canada demonstrated, parliamentary coordination can harmonise departmental mandates without demanding constitutional overhaul. Through intelligence-sharing protocols, cross-departmental threat tagging and mandate convergence under the Cabinet Office, the UK can build an integrated response framework that respects departmental specialisation while overcoming its fragmentation.

The Canadian experience is especially salient given Westminster-system similarity. The UK does not need to rewrite ministerial responsibilities – it must reconceive how those responsibilities are activated and aligned in the face of non-linear threats.

III. Enabling Legal Bureaucratism – Without Judicial Overreach

Legal frameworks must shift from isolated application to layered enforceability. The United States demonstrates how overlapping authorities – terrorism designation, sanctions, immigration law – can operate in parallel without legal confusion. While the UK lacks equivalent executive direction, it can pursue multipoint designation through existing legislature, while developing novel adaptable legislature:

Terrorism Act 2000: full organisational proscription;

Sanctions and Anti-Money Laundering Act 2018: financial disruption of networked affiliates;

Immigration and Asylum Acts: exclusion of affiliated individuals;

National Security Act 2023: counter-influence regulation.

These instruments already exist. What is currently lacking is strategic doctrine that links them in sequence – turning law into an operational web.

IV. Narrative Legitimacy and Civic Immunity

The policy must be communicated not as a foreign policy escalation, but as a public protection measure. Sweden's strategic use of narrative – portraying proscription as a defence of domestic civic space – demonstrated how legal action can be insulated from diplomatic escalation. This is not a rhetorical issue. Narrative framing determines whether policy is seen as coercive or protective, and therefore whether it retains political consensus across electoral cycles.

Community engagement will be central. Proscription must not alienate, but shield diaspora communities from ideological coercion. This approach transforms the policy from a deterrent into a defence mechanism – restoring trust in the state's capacity to protect citizens from transnational pressure.

V. A Living Framework, Not a Static Architecture

The nature of hybrid threats demands adaptation, not finality. The doctrine must include mechanisms for revision – structured intelligence feedback loops, inter-agency after-action reporting and regular parliamentary review. Policy must evolve not only with emerging threats, but with the tactics of adversaries who adapt to the very enforcement mechanisms intended to stop them.

This does not mean perpetual overhaul. It means embedding institutional elasticity: the ability to adjust policy interpretation, operational priority and enforcement coordination without legislative paralysis.

Conclusion – Strategic Alignment, Not Strategic Expansion

This blueprint does not prescribe new agencies, new statutes or new political declarations. It proposes a reconfiguration of how the UK sees threat, how it aligns capability and how it projects security domestically and internationally. What is required now is not invention, but recognition – that the structures inherited from an earlier threat era are being exploited by adversaries such as the IRGC, fluent in institutional blind spots.

Sweden, Canada and the United States each chose strategic alignment over institutional scale. The UK can do the same. But it must begin with one foundational step: treating the hybrid actor not as an anomaly, but as the new normal. Only then can the UK build a security doctrine equal to the complexity of the threat it now faces.

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org