Small Wars & Insurgencies

ISSN: 0959-2318 (Print) 1743-9558 (Online) Journal homepage: www.tandfonline.com/journals/fswi20

The Islamic Republic of Iran's use of criminal intermediaries for extraterritorial assassinations and covert violence: a gray zone strategy of outsourced repression

Ardavan M. Khoshnood

To cite this article: Ardavan M. Khoshnood (2025) 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, 1433-1461, DOI: 10.1080/09592318.2025.2555583

To link to this article: https://doi.org/10.1080/09592318.2025.2555583

Published online: 03 Sep 2025.

SMALL WARS & INSURGENCIES
2025, VOL. 36, NO. 8, 1433–1461
https://doi.org/10.1080/09592318.2025.2555583

Routledge
Taylor & Francis Group

The Islamic Republic of Iran's use of criminal intermediaries for extraterritorial assassinations and covert violence: a gray zone strategy of outsourced repression

Ardavan M. Khoshnood

Department of Clinical Sciences Malmö, Lund University, Malmö, Sweden

ABSTRACT

The Islamic Republic of Iran (IRI) has employed assassinations and proxy violence as tools of statecraft. Dissidents in exile have been killed, targeted, or systematically threatened, while Israeli-linked entities across Europe have faced repeated attacks. In recent years, Tehran has increasingly outsourced these operations to state-linked criminal intermediaries. This paper analyzes Iran's approach through the lens of Gray Zone Strategy, showing how criminal outsourcing extends Tehran's reach, preserves deniability, and enables coercion below the threshold of open conflict. These hybrid tactics blur the boundaries between organized crime, terrorism, and state repression – posing urgent challenges for Western legal, intelligence, and security frameworks.

ARTICLE HISTORY Received 10 May 2025; Accepted 19 August 2025

KEYWORDS Iran; Islamic Republic of Iran; terrorism; assassination; gray zone strategy; criminal gangs; criminal intermediaries; counterintelligence

1. Background

Since its establishment in 1979, the Islamic Republic of Iran (IRI) has engaged in extensive covert operations targeting opponents and foreign adversaries abroad. These have included espionage, sabotage, terrorism, and more than 160 documented assassinations of dissidents living in exile.[1] Despite repeated accusations by opposition groups and international law enforcement, the regime has consistently denied involvement. In many instances, it even blamed rival opposition factions; maintaining this narrative even when individuals linked to the regime were arrested or convicted.[2] This pattern reflects the strategic logic of *Gray Zone Strategy* (GZS), wherein states pursue coercive

CONTACT Ardavan M. Khoshnood ardavan.khoshnood@med.lu.se Department of Clinical Sciences Malmö, Lund University, Clinical Research Centre, CRC 91-12, Malmö SE-202 13, Kingdom of Sweden

objectives through covert means while maintaining plausible deniability. By pairing political violence with sustained ambiguity, gray zone operations allow the perpetrator to achieve results without provoking direct confrontation or legal consequences.

Revelations in early 2025 forced a reassessment of the regime's denials. On March 8, Brigadier General Mohsen Rafighdoust, former Minister of the Islamic Revolutionary Guard Corps (IRGC), gave a bombshell interview to the Iranian platform *Didban Iran*.[3] He admitted to organizing a series of assassinations in Europe, including those of Prince Shahriar Shafiq in 1979, General Gholam Ali Oveisi in 1984, Dr. Shapour Bakhtiar in 1991, and Dr. Fereydoun Farrokhzad in 1992. He also confirmed the IRGC's involvement in a failed 1980 attempt against Bakhtiar, carried out by Lebanese operative Anis Naccache.

More strikingly, Rafighdoust disclosed that several of these killings were outsourced to hired Basque separatists, coordinated via intermediaries including an Egyptian cleric based in Germany. The cleric also facilitated payment, enabling a multilayered structure that shielded Iranian officials from direct attribution. This early example of non-ideological outsourcing revealed the regime's willingness to employ criminal networks to achieve strategic ends.

Further operational details emerged in a previously unreleased 2018 interview with Rafighdoust, broadcast only after his 2025 statement.[4] He revealed that the IRGC maintained a covert bank account at *Bank Saderat Iran*[5] in Frankfurt, used to discreetly fund overseas operations outside official budgets. According to Rafighdoust, deposits into the account often came from untraceable sources, including informal 'bonuses' secured during arms deals.

These disclosures directly implicate senior Iranian officials in ordering and financing political assassinations abroad. They also shed light on the structural mechanisms that enable these operations: outsourcing, compartmentalization, and financial obfuscation. The regime's evolving reliance on criminal intermediaries, especially since 2010, suggests a calculated shift in its doctrine of repression. This transformation raises key questions about Iran's strategic objectives, the logic behind its extraterritorial campaigns, and the vulnerabilities it exploits in Western counterintelligence systems.

This paper builds on existing documentation of Iran's extraterritorial operations – most notably Levitt's empirical mapping,[6] by offering a conceptual analysis of outsourcing as a structural feature of its GZS. Rather than merely cataloging incidents, the paper explains how Iran employs hired intermediaries, often non-ideological or criminal actors, not only to evade attribution but to fragment opposition, create reputational ambiguity, and exert coercion below the threshold of conventional conflict. This analysis draws from – but goes beyond – existing empirical work by situating outsourcing within a broader framework of cloaked coercion. In

support of this argument, the paper also incorporates a major public admission by former IRGC Minister Mohsen Rafighdoust, who openly acknowledged the regime's responsibility for extraterritorial assassinations and the outsourcing of such missions to foreign actors. While brief, this unprecedented confession marks the first public acknowledgment by a senior Iranian official of the state's direct role in outsourcing political violence abroad.

Second, the paper contributes to gray zone literature by clarifying how non-state criminal organizations can function as strategic extensions of state violence. It introduces a conceptual framework that distinguishes Iran's consistent, structured use of intermediaries from ad hoc or opportunistic collaboration. These actors operate without ideological loyalty yet are embedded within the regime's coercive apparatus – acting as surrogate or auxiliary agents in a deniable architecture of state repression.

2. Theoretical framework: gray zone strategy

To analyze this strategic evolution, it is necessary to define the core principles of GZS and situate the IRI's behavior within this conceptual framework. Rather than relying solely on conventional military power, gray zone operations emphasize covert, incremental, and unacknowledged actions that enable states to advance their interests without provoking direct confrontation. The U.S. Central Intelligence Agency[7] defines covert action as 'an operation designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the sponsoring power; it may include political, economic, propaganda, or paramilitary activities'. Covert action is a widely employed foreign policy tool, used by many states across a range of contexts. However, while covert actions can occur independently, they may also serve as key instruments within a broader gray zone strategy. GZS encompasses a wider array of coercive behaviors – covert, ambiguous, and incremental – designed to achieve strategic objectives below the threshold of open conflict. In this paper, the term *covert action* is used specifically to denote such actions when employed as part of Iran's GZS.

GZS serves as a complementary theoretical lens by highlighting the strategic use of ambiguity, hybrid instruments, and attribution avoidance as tools of statecraft. In the Iranian context, this lens reveals how contracted operations, especially through criminal intermediaries, embodies calibrated coercion that avoids overt escalation. This paper adopts the definition of GZS as formulated by the RAND Corporation:

> An operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt

> a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events.[8]

According to RAND, gray zone campaigns typically exhibit eight interrelated characteristics: (I) they remain below the threshold that would trigger a military response; (II) they unfold gradually over time; (III) they involve ambiguous actions, complicating accountability; (IV) even when attributable, they are framed with legal or political justifications to obscure violations; (V) they avoid threatening the target's vital interests to reduce the risk of retaliation; (VI) they leverage the implicit risk of escalation for coercive effect; (VII) they rely on nonmilitary or hybrid tools; and (VIII) they exploit societal and institutional vulnerabilities within the target state.[9] Collectively, these traits allow state actors to pursue ambitious strategic objectives through sustained coercion while avoiding the risks of open warfare.[10]

Each of these dimensions is observable in the IRI's extraterritorial operations, particularly in its recurring use of state-linked criminal intermediaries whose involvement remains obscured to exert coercive pressure abroad. While Iran has long demonstrated pragmatism in its choice of intermediaries – including non-ideological actors like criminal groups and foreign militants – what is increasingly evident is the systematic integration of this practice into a broader gray zone strategy. Rather than improvisation, the use of criminal intermediaries now reflects a more structured approach shaped by modern constraints such as heightened surveillance, diplomatic costs, and restricted access for official operatives. In this sense, Iran's reliance on opaque, coercive, and deniable methods aligns with GZS not only in form but in strategic function.

Mazarr emphasizes that gray zone strategies are particularly attractive to 'measured revisionist' states that benefit from and depend on the international order, yet seek to transform aspects of it in their favor. For these actors, opacity and patience become core instruments: they proceed incrementally through what Mazarr calls strategic gradualism, leveraging non-military pressure, and covert tools to advance revisionist aims while avoiding escalation thresholds.[11] Yet, the concept of GZS is not without challenges. As Brands[12] argues, GZS often risks conceptual overreach, with the term stretched so far that it includes everything short of war and thus loses analytical clarity. He emphasizes that to be useful, GZS must be constrained to cases of calculated, below-threshold coercion with gradualist and revisionist intent. Otherwise, the term risks conflating unrelated forms of irregular conflict. Brands identify a central paradox: GZS is both ambiguous and strategic; designed to operate under the radar while still achieving traditional warlike objectives.

These theoretical insights, on both the strategic logic and conceptual boundaries of GZS, provide a useful lens for analyzing the IRI's behavior in the international arena. As a revisionist actor, the IRI has repeatedly turned to

gray zone tools to expand regional influence and suppress dissident threats abroad. The regime employs assassinations and hired violence as deliberate tools of gray zone coercion to suppress dissent abroad while avoiding attribution. The regime's extraterritorial assassinations fall into two broad categories: dissident targets and adversary-linked targets like Israeli individuals. Attacks on adversary-linked targets are more clearly aligned with classic gray zone objectives; avoiding escalation, maintaining deniability, and projecting coercive pressure onto rival states. By contrast, assassinations of dissidents, while rooted in regime preservation, also serve a strategic, performative function when conducted abroad. These operations project power into hostile environments, expose the vulnerabilities of host-state protection, and intimidate both diaspora communities and foreign governments. In this sense, dissident killings function as both instruments of domestic control and tools of external signaling. Differentiating between these logics – coercive deterrence versus coercive intimidation – clarifies how Iran's outsourced violence operates across multiple strategic registers within its gray zone playbook.

GZS, thus, enables actors like Iran to challenge the international order without inviting direct confrontation.[13] This logic underpins the IRI's evolving strategy of hiring non-state intermediaries for covert operations.

In the broader literature on proxy warfare and state – non-state cooperation, scholars have developed typologies to classify these relationships. Rauta offers a four-part distinction between proxies, auxiliaries, surrogates, and affiliated forces, classified by degrees of autonomy, ideological alignment, and organizational integration.[14] This current paper focuses on the latter two categories – surrogates and affiliated forces – as most appropriate for describing the types of criminal actors employed by the IRI in its extraterritorial operations. These actors are not ideologically aligned with Iran but are embedded functionally in its coercive infrastructure through transactional cooperation. I refer to these actors as *state-linked criminal intermediaries*: non-ideological, deniable agents used by the IRI for coercive operations without direct state attribution. These state-linked criminal intermediaries are typically profit-driven actors from local or transnational organized crime networks, engaged by the IRI on a transactional basis for specific missions. While many engagements are short-term and mission-specific, others develop into recurring arrangements sustained by mutual utility, protection, or financial reward.[15] Unlike full proxies such as Hezbollah, these intermediaries are recruited for specific missions where attribution avoidance and local access are paramount. Their value lies in providing operational discretion and strategic insulation while advancing regime objectives. Framing them as *state-linked criminal intermediaries*, rooted in Rauta's surrogate and affiliated force typology, clarifies how the IRI's use of organized crime represents not ad hoc improvisation, but a deliberate evolution in its gray zone toolkit.

While deniability is a core feature of GZS, it does not, on its own, explain the IRI's turn to criminal intermediaries. After all, Iran has consistently denied involvement in extraterritorial assassinations for decades. The shift to criminal actors reflects a functional adaptation to operational constraints. In Western contexts, Iran faces intelligence and operational constraints: limited local networks, linguistic and cultural barriers, surveillance of known proxies, and visa restrictions. Criminal groups offer local access and logistical support that official operatives often lack.[16] Their utility lies not just in masking state involvement, but in enabling operations that would otherwise be infeasible.

While Tehran has long relied on ideological proxies such as Hezbollah, its methods have increasingly evolved to incorporate pragmatic arrangements with non-ideological actors including European-based criminal networks.[17] These state-linked criminal intermediaries are tasked with sensitive operations such as assassinations, allowing the regime to preserve strategic standoff and avoid attribution. As Jordán observes, the use of such intermediaries is central to GZS as it enables aggressors to obscure attribution, fragment accountability, and reduce the risk of direct retaliation.[18] In the case of the IRI, this model permits the regime to exert coercive pressure abroad while avoiding overt military engagement or diplomatic fallout.[19]

Carment and Belo[20] add that non-democracies, like Iran, are more disposed to gray zone operations due to their centralized, flexible decision-making structures. They face fewer institutional constraints and can exploit ambiguity, often outsourcing disruptive acts to criminal or paramilitary proxies while denying involvement. This complicates attribution, especially in democracies with high legal thresholds.

Furthermore, for regimes facing militarily stronger adversaries, gray zone strategies offer a means 'to manage risk, limit escalation, and avoid war', without engaging in direct conflict.[21] The IRI's outsourcing of violence is thus not merely an act of deflection; it is a method of asymmetric statecraft. By relying on criminal intermediaries, the IRI applies pressure without exposing itself to direct retaliation while achieving strategic objectives. It is important to emphasize that this evolution does not represent a replacement of ideological proxies such as Hezbollah, but rather a diversification of operational tools. The IRI's core strategic goals – regime survival, deterrence, and extraterritorial repression – have remained constant. What has changed is the regime's growing willingness to delegate certain missions to intermediaries when concealment, flexibility, or local access are prioritized over ideological loyalty.

This adaptive approach also reflects structural shifts in the international environment, including the globalization of finance, advances in communication technologies, and the diffusion of non-state violent capabilities. In this context, the turn to criminal intermediaries should be understood as

a functional expansion within an existing strategic logic, not a fundamental change in Iran's objectives.

Moreover, the operational environments in which the IRI acts – particularly Western democracies – are especially vulnerable to GZS. As Braw[22] argues, gray zone tactics are especially effective against Western countries because of their open societies, limited state control, and permissive environments for civilian and business activity; conditions that adversaries can exploit for non-military coercion. The IRI has capitalized on these vulnerabilities in ways that echo the gray zone playbooks of other revisionist powers. While not as institutionalized as Russia's hybrid warfare apparatus or China's state-linked influence networks, the IRI's methods reflect a similar logic: the strategic use of covert proxies, criminal intermediaries, and operations designed to obscure state involvement to advance national interests without triggering open conflict.[23] Thus, when analyzed through the lens of GZS, this behavior emerges as part of a broader pattern: calculated, coercive, and deliberately designed to fall short of war while still shaping the strategic environment in Tehran's favor.

Finally, following Hoffman's[24] insights, it is essential to note that gray zone campaigns are not just collections of tactics, rather, they are strategic endeavors guided by an internal logic or 'theory of success'. Iran's use of covert and state-linked criminal intermediaries demonstrates a rational hypothesis: that it can manipulate foreign environments, deter opposition, and enforce regime interests abroad while avoiding overt conflict, minimizing backlash, and preserving cover.

Taken together, these theoretical perspectives provide a coherent framework for analyzing Iran's evolving strategy. GZS offers the structural logic: calibrated ambiguity, below-threshold coercion, and sustained strategic intent. Rauta's typology helps specify the role of criminal intermediaries within this system as surrogates or affiliated forces. Mazarr's concept of strategic gradualism and Hoffman's theory of success explain the long-term design and internal coherence of these campaigns. Meanwhile, Carment, Belo, and Braw illuminate the institutional and environmental conditions that make gray zone strategies especially appealing and effective for authoritarian regimes like Iran. In sum, GZS is especially suitable for analyzing the IRI's behavior because it captures how Tehran leverages ambiguity, operational cover, and hybrid tools – including criminal intermediaries – to advance state objectives without inviting direct confrontation.

In addition to strategic calculation, Iran's approach to gray zone statecraft is also shaped by a distinct ideological logic rooted in the post-revolutionary worldview of the Islamic Republic. While diplomatic platforms and financial cover enable operational capacity, ideology shapes how the IRI selects targets and legitimizes repression. Domestic ideological factors thus play a reinforcing role. Khomeini's legacy of 'Westoxification' and the oppressed-

oppressor narrative fosters a siege mentality, wherein exiled opposition figures are seen not merely as political adversaries but as agents of hostile foreign powers.[25] In this worldview, dissidents are internal enemies with external sponsors, justifying their elimination as an act of regime preservation. This ideological framing turns targeted assassinations into acts of 'defensive offense', aligning violence with both strategic calculation and theological justification.

3. Iran's extraterritorial violence: strategic logic and gray zone practice

Since its establishment in 1979, the IRI has used targeted assassinations and acts of political violence.[26] These operations have been aimed at eliminating opposition figures, intimidating diaspora communities, and asserting Tehran's extraterritorial reach. Far from sporadic or reactive, this campaign of global assassinations and covert violence is a calculated extension of the regime's internal repression, carefully planned and coordinated at the highest levels of Iran's security apparatus.[27]

As discussed earlier, the regime's post-revolutionary campaign began with the assassination of Prince Shahriar Shafiq in 1979—an operation emblematic of Iran's early use of ideologically motivated violence directly sanctioned by revolutionary elites.[28]

Iran's use of extraterritorial violence is both strategic and methodologically sophisticated. A defining feature of the regime's modus operandi is its use of deception to infiltrate exile communities. Iranian operatives often pose as fellow dissidents or sympathizers, a 'Trojan horse' tactic that enables both surveillance and psychological warfare. By sowing distrust and suggesting that assassinations stem from internal disputes, the regime fractures opposition movements.[29] These tactics not only enable operational success but also erode collective resistance, aligning with GZS goals of fragmented opposition and reputational ambiguity.

As with other early cases, the 1984 assassination of General Gholam Ali Oveissi in Paris – claimed by a group calling itself Islamic Jihad – demonstrated the regime's early reliance on loosely affiliated fronts to obscure its involvement and diffuse responsibility.[30]

This early phase of extraterritorial violence spanning from 1979 to the early 1990s was marked by ideological justification and revolutionary fervor, often executed by regime-aligned militants. Tehran, however, has increasingly turned to criminal networks to target opponents in Western countries. These operations involve the use of covert, non-military tools to undermine adversaries while staying below the threshold of open war.[31] Decentralized security structures and legal frameworks in Western states create vulnerabilities that actors like Iran can exploit.[32] It is precisely these vulnerabilities –

legal, institutional, and societal – that state-linked criminal intermediaries are designed to exploit on Tehran's behalf.

The 1991 assassination of Dr. Shapour Bakhtiar marked the peak of Iran's early, centrally directed extraterritorial violence. These operations, characterized by infiltration, forged documentation, and coordination across multiple state bodies, reflected a maturing infrastructure of covert action.[33] Yet their visibility and diplomatic consequences were increasingly difficult to contain. This became undeniable in 1992, when IRI operatives assassinated Iranian opposition leaders at the Mykonos restaurant in Berlin. The resulting trial marked a watershed moment: for the first time, a European court formally identified Iran's senior leadership, including Supreme Leader Ali Khamenei, as responsible for ordering the killings. The diplomatic backlash was severe, leading to the recall of European ambassadors and a major rupture in Iran's relations with the EU.[34]

In response, Tehran recalibrated. While assassinations remained part of its toolkit, the regime increasingly turned to more deniable tactics – overt intimidation, arson, surveillance, and cyber-enabled disruption.[35] These post-Mykonos adaptations reflect continuity in intent – coercion, deterrence, and projection, but a shift in method. Rather than overt action, Iran began operating more squarely within the logic of gray zone strategy: calibrated violence, strategic ambiguity, and plausible deniability designed to achieve regime objectives while minimizing diplomatic fallout.

3.1 Operational evolution and gray zone practice

3.1.1 From ideological proxies to criminal surrogates

Rafighdoust's acknowledgment of hiring Basque separatists in the 1980s and 1990s, and more recent evidence[36] of the regime hiring state-linked criminal intermediaries, illustrate how Iran recalibrates methods to lower visibility even more than before. This marks a turning point in Iran's GZS; from ideologically aligned proxies toward for-profit criminals who offer greater concealment and access. An early example of this transition occurred in 2011, when Qods Force[37] operatives attempted to contract a violent drug cartel to assassinate the Saudi Ambassador to the United States.[38] The plan unraveled when the supposed intermediary turned out to be a DEA informant. The operative, Mansour Arbabsiar – a U.S. citizen – was sentenced to 25 years in prison, and several Qods Force officers, including then-commander Qassem Soleimani, were sanctioned for their roles.[39] This operation was one of the first to reveal Iran's willingness to contract non-ideological, criminal actors for sensitive extraterritorial missions.

Yet the nature of these relationships demands conceptual precision. Referring to them as 'partnerships' risks implying parity, whereas Iran's use of these actors is far more hierarchical and instrumental. The state selects,

deploys, and discards such intermediaries as needed, leveraging them to create standoff, ambiguity, and deniability in alignment with its broader GZS.[40] As outlined in the theoretical framework, these criminal intermediaries correspond to what Rauta classifies as surrogates or affiliated forces[41]: externally recruited, non-ideological, and operationally useful actors who remain subordinate to the state's strategic objectives. This outsourcing is not improvised – it is a structured component of Iran's gray zone statecraft, offering efficiency, cover, and reach.

The IRI's outsourcing of violence to criminal networks is neither random nor purely opportunistic. Selection appears to follow a pragmatic logic of access, chances of success, and attribution avoidance. In several documented cases, intermediaries have included individuals of Iranian or non-Iranian origin embedded in local criminal ecosystems.[42] These actors are often culturally fluent, legally resident, and able to blend into target environments, making them ideal for tasks requiring both discretion and reach.

From a counterintelligence perspective, these relationships offer both operational benefits and systemic vulnerabilities. Criminal organizations can provide covert violence, access to forged documents, and transnational mobility.[43] But, they are also volatile, financially motivated, and subject to external infiltration. Iran's ability to spot, assess, develop, and handle such actors likely draws on a mix of diaspora monitoring, indirect vetting through intermediaries, and the regime's long-standing experience in clandestine operations.[44] Termination of relationships appears similarly instrumental: when actors are arrested, disavowal follows; when operations fail, accountability is obfuscated.[45]

3.1.2 Case Studies and criminal infrastructure

While the shift to criminal intermediaries marks a significant evolution in Iranian practice, it is not unique. Other regimes – including Russia,[46] North Korea,[47] and even some Western states[48]—have similarly employed criminals to advance covert foreign policy objectives. However, the Iranian case reflects a distinct synthesis of ideological motivation and instrumental outsourcing. Unlike Russia's incorporation of organized crime into a mafioso-style hybrid warfare model,[49] or North Korea's use of cybercrime primarily for revenue generation and sanctions evasion,[50] Iran's approach centers on both regime protection and extraterritorial repression through the strategic use of criminals.

What distinguishes the IRI is not only its operational reliance on criminal actors, but the way it embeds these relationships into a coherent gray zone doctrine. This strategy calibrates risk through layered ambiguity, using criminal intermediaries to reduce visibility, fragment responsibility, and complicate legal and diplomatic responses, particularly in liberal democracies where evidentiary thresholds for attribution are high.

(1) *Chronological Expansion of Criminal Outsourcing*. Multiple assassination and kidnapping attempts – such as the abduction of Habib Chaab and the murder-for-hire plot against a U.S.-based dissident – illustrate how the IRI contracts lethal operations to obscure its role and expand its reach.[51] The 2015 assassination of Mohammad Reza Kolahi in the Netherlands, carried out by a cocaine trafficker later convicted in Dutch court, is a prominent example. Though formal attribution remained elusive, Dutch intelligence (AIVD[52]) later stated there were 'strong indications that Iran was involved'.[53] This trend becomes even more pronounced in the years that followed. From 2017 to 2021, both the Ministry of Intelligence (MOI) as well as the IRGC increasingly relied on the Iranian narcotics trafficker Naji Ibrahim Sharifi Zindashti as a trusted ally. Zindashti and his network were implicated in the Istanbul assassinations of media executive Saeed Karimian (2017)[54] and cybersecurity defector Masoud Vardanjani (2019).[55] In 2020, the same network facilitated the abduction of Habib Chaab, a leader of the terrorist-separatist organization Arab Struggle Movement for the Liberation of Ahvaz,[56] through a honey trap operation, leading to his execution in Iran.[57] The pattern continued in 2021, when Zindashti's operatives recruited members of the Canadian Hells Angels to plan assassinations of regime opponents.[58] Though the attempt failed, it revealed how Iran uses global criminal actors to operationalize violence with minimal attribution risk. These events mark the institutionalization of criminal outsourcing as a recurring mechanism for high-risk missions. Levitt[59] corroborates this pattern, documenting over 116 unique external operations since 2020, many of which involve local criminals, drug traffickers, and organized crime figures acting as operational surrogates. The inclusion of figures like Zindashti and transnational biker gangs in multiple assassination and surveillance plots illustrates the operational infrastructure Iran has built beyond its ideological networks.

(2) *European Operations and Diversified Networks, 2022–2025*. This model has since expanded further across Europe. In late 2022, *Der Spiegel* uncovered a sprawling IRI-linked operation involving surveillance, arson, and coordinated violence against Jewish and Israeli targets.[60] It began with Babak, a German-Iranian with a violent criminal record, who threw a Molotov cocktail at a school in Bochum, believed by investigators to have mistakenly targeted the wrong building, as a synagogue was located nearby. The same night, gunfire struck a rabbi's residence in Essen. The operation widened in early 2023, when Abdelkrim ('Krimo'), a 34-year-old French citizen of Algerian origin with a background in Marseille's drug wars, arrived in Berlin. He conducted surveillance on Jewish institutions, tracked a lawyer

representing Israeli clients, and was later found to be acting on instructions from an inmate in a French prison. Coordination appeared to stem from Ümit, a Lyon-based drug trafficker with multiple fake identities, believed to be residing in Iran under IRI protection. These decentralized, covert actors illustrate how Iran uses hardened European criminals to penetrate open societies and exert covert pressure while avoiding conventional escalation.

The same network was linked to an Iranian former Hells Angels boss, Ramin Yektaparast, accused of a gruesome murder in Germany, who fled to Iran and was believed to be assisting attacks on Jewish and Israeli targets prior to his reported death in early 2023. The campaign escalated further: between 28 December 2023, and 3 January 2024, four Israeli-linked businesses in southern France were set ablaze. All addresses were later found on Krimo's phone, reinforcing the coordinated nature of the operation.

Meanwhile, in Sweden and Denmark, a string of incidents raised alarms throughout 2024. In January a suspected grenade was discovered inside the Israeli embassy in Stockholm, followed by gunfire outside the embassy in May and October. In October, shots and explosions occurred near the Israeli embassy in Copenhagen as well. Though Danish officials have not confirmed the embassy was the target, Swedish intelligence sees the incidents as part of a broader Iranian pattern.[61]

These cases underscore a shift from ideological proxies to multiethnic criminal networks embedded across Europe, used to carry out covert gray zone operations against dissidents and Israeli-linked targets. The reliance on ethnically diverse intermediaries – such as Krimo (Algerian-French), Babak (Iranian-German), Ümit (Turkish or Kurdish), and Yektaparast (Iranian-German) – adds layers of ambiguity that hinder attribution, obstruct prosecution, and strain diplomatic response. This operational diversity frustrates conventional counterintelligence approaches and exemplifies how the IRI has evolved its gray zone strategy into a decentralized, criminally outsourced system of targeted coercion.

3.1.3 Diplomatic platforms, financial channels, and strategic synthesis

While criminal outsourcing provides the tactical manpower, diplomatic and financial platforms provide the strategic infrastructure for Iran's gray zone campaigns. One critical tool in this strategy is the IRI's systematic use of diplomatic missions. Historical evidence such as the Mykonos case in 1992, the expulsions of Iranian diplomats in Europe for involvement in assassination plots, and more recent incidents like the 2018 case of Iranian diplomat Assadollah Assadi reveal how operatives working under diplomatic cover smuggle explosives, carry out reconnaissance, and coordinate attacks.[62] Assadi, a senior officer of the Ministry of Intelligence stationed in Austria,

exploited his diplomatic immunity to transport explosives and orchestrate a planned attack on an opposition rally in Paris. Assadi relied on intermediaries to execute the plot, allowing the state to maintain cover. This case, among others, is featured prominently in Levitt's interactive map, which highlights the dual-use nature of Iran's diplomatic corps in both operational planning and logistical facilitation.[63] The data reveal that diplomatic immunity continues to serve as a core enabler in Iran's outsourced coercion model. Moreover, diplomatic immunity shields state actors from consequences, reinforcing the ambiguity central to Iran's strategy. The 1992 murder of Dr. Fereydoun Farrokhzad in Germany – denied by Hossein Mousavian, IRI's ambassador to Germany at the time[64]—was later confirmed by Brigadier General Mohsen Rafighdoust to have been ordered by the regime.[65] Such cases demonstrate the dual utility of diplomatic platforms: not only to mask covert operations but also to deflect accountability through categorical denials.

3.1.3.1. Financial Channels and Operational Cover. States systematically select non-state actors – ranging from extremist groups to for-profit criminal intermediaries – as covert tools of foreign policy.[66] By leveraging criminals with little ideological allegiance, Iran operates through carefully orchestrated financial channels – such as unregistered or clandestine bank accounts in Europe – to pay assassins.[67] Financially, these operations are supported through opaque channels including cash smuggling, money laundering, shell companies, and front organizations often tied to the IRGC and MOI.[68] State-affiliated charitable foundations (*bonyad* in Farsi) and businesses provide additional cover, allowing the regime to sustain operations while avoiding financial scrutiny.[69] These economic instruments extend the regime's reach into European jurisdictions while maintaining formal distance from state structures.

These tactics enable long-term operational continuity, supporting criminal intermediaries while complicating sanctions enforcement and legal tracking. What emerges is a rational theory of coercion under constraint: when direct confrontation is too costly, the IRI blends proxies, diplomats, and financial tools to coerce without attribution.

From the assassination of Prince Shahriar Shafiq in 1979 and the 1984 murder of General Gholam Ali Oveisi to the wave of covert plots across Europe between 2022 and 2025, the IRI's methods have evolved but consistently reflect a gray zone model of state violence. The shift from early IRGC-led revolutionary fervor to modern criminal outsourcing illustrates both strategic adaptability and enduring reliance on ambiguity. Viewed through the GZS lens, Iran's approach becomes clearer: the regime pursues core objectives – protecting itself, deterring opposition, and projecting influence – while remaining below the threshold of war through a blend of covert operatives, unacknowledged intermediaries, and insulated infrastructure.

3.2 Strategic logic and ideological justifications

The IRI views the elimination of exiled opponents as serving three strategic goals: removing symbolic leaders, instilling fear, and asserting extraterritorial reach. Such actions are interpreted internally as preemptive self-defense. This framing narrows the moral and political space for dissent, portraying opposition not as domestic disagreement but as external subversion. The regime views the cost of contracted killings as an acceptable price for maintaining domestic loyalty, deterring organized resistance, and reinforcing the perception that exile offers no safety from retribution.

3.2.1 Coercive signaling and iterative adaptation

Beyond the immediate tactical gain of neutralizing individuals, extraterritorial attacks are used for deterrence and signaling. High-profile killings function as violent messages intended to discourage activism, fragment opposition, and remind audiences, both domestic and foreign, of the regime's reach.[70] Symbolic targets, brutal methods, and transnational reach serve not only to punish but to warn. Even non-lethal attacks like arson, threats, and bomb plots, function as coercive warnings, often delegated to criminal surrogates. They also allow Tehran to test the response thresholds of Western governments without crossing lines that would provoke a robust diplomatic or military response. This iterative approach enables the Islamic Republic to continuously refine its gray zone tactics. By observing which operations draw condemnation, sanctions, or criminal prosecution – and which do not – the regime calibrates future operations for maximum effect and minimal consequence. The regime actively probes legal, political, and intelligence red lines, learning from each engagement how to operate more effectively in the zone of tolerated ambiguity. State-linked criminal intermediaries are particularly suited to this probing function, allowing the state to test limits without direct exposure.

The 1994 bombing of the AMIA[71] Jewish center in Buenos Aires exemplifies how this strategy can escalate. Though Tehran denies involvement, Argentine prosecutor Alberto Nisman[72] presented extensive evidence implicating Iran's Qods Force, prompting Interpol warrants for several senior Iranian officials.[73] This incident marked a shift from targeting individual dissidents to striking symbolic institutions tied to geopolitical adversaries, particularly Israel.

3.2.2 Criminal outsourcing as strategic optimization

The IRI's systematic use of criminal intermediaries is not merely a matter of convenience or cover. Rather, it is a strategic optimization of coercive capacity under constraint. The regime faces real limits: it cannot afford symmetrical conflict with more powerful states, and official operatives are

increasingly subject to international surveillance and sanctions. This strategic environment makes covert outsourcing a rational adaptation: it enables projection of force without escalating confrontation. By turning to local criminals, Iran secures operational benefits: cultural familiarity, logistical expertise, and reduced risk of infiltration. Their actions serve Iranian interests while maintaining a firewall between the operation and official institutions.

Iran is not inventing this model in a vacuum, it draws on established hybrid actors whose dual roles offer lessons for strategic outsourcing. Hezbollah offers a template for this logic. Though ideologically aligned and state-sponsored, Hezbollah has long collaborated with criminal actors in drug trafficking, smuggling, and financial schemes.[74] This blending of ideological and instrumental motives provides a precedent for Iran's wider use of criminal outsourcing.

Tehran's brazen operations, sometimes outsourced through criminal rings, display an ability to bypass host-country security through local surrogates and warn external states that hosting or backing Iranian dissidents might incur heavy costs.[75] This deterrent logic is reinforced by the regime's method of execution. Rather than relying solely on official operatives, the IRI systematically turns to criminal surrogates who offer operational reach while keeping the state insulated.[76] While Iran's clerical establishment retains centralized control over targeting, operational specifics, that is acquiring weapons, conducting surveillance, and carrying out the hit, are delegated to criminals who know the terrain, or as previously seen to its diplomatic missions.[77]

State-backed groups have increasingly recognized the strategic value of engaging with illicit networks for tasks such as smuggling, money laundering, and targeted violence.[78] Hezbollah's collaboration with criminal actors illustrates how such partnerships can offer operational advantages even when robust state sponsorship is available.[79] Iran follows a similar logic.

3.3 Policy implications and security responses

3.3.1 Structural challenges and institutional blind spots

The IRI's use of state-linked criminal intermediaries poses a structural challenge to Western law enforcement and intelligence services, which are often unprepared for hybrid threats that merge state objectives with non-state execution. As Belli et al.[80] observe in relation to Hezbollah, illicit operations often blur the line between terrorism and profit-driven crime, complicating distinctions between ideological and criminal actors. The same analytical confusion now hampers efforts to counter Iran's outsourced coercion.

Iran's increasing use of similar hybrid tactics demands a recalibrated response. Western agencies must treat criminal webs tied to the IRI as national security threats, rather than merely as organized crime groups. This

requires real-time intelligence-sharing – both nationally and internationally – since criminal actors operate seamlessly across jurisdictions. Democratic legal systems, designed to protect civil liberties, are often exploited by hostile regimes operating through criminal proxies.[81] Closing legal blind spots and building centralized investigative bodies that merge terrorism and organized crime units can help bridge existing enforcement gaps.[82] These structural adjustments are essential to confront the hybrid character of Iranian gray zone operations.

A particularly vulnerable node in this system is the diplomatic infrastructure Iran exploits. Repeated plots involving Iranian diplomatic missions show that embassies often serve not just as diplomatic outposts but as protected hubs for planning, financing, and executing extraterritorial repression.[83] The 2018 case of Iranian diplomat Assadollah Assadi, highlights this dual-use function. Diplomatic immunity has become one of the regime's most effective shields against accountability.

To respond, Western states should consider reducing Iran's diplomatic footprint, expelling officials credibly linked to covert activity, and proactively monitoring consulates suspected of enabling repression. Western countries should also update their legal frameworks to ensure that foreign-directed surveillance, intimidation, or harassment of exiles is prosecuted as a national security issue – not treated as petty crime or isolated harassment. Crafting laws that explicitly criminalize foreign-directed repression would allow law enforcement to address such incidents as patterns of hostile state activity. Without these legal and diplomatic reforms, the IRI will continue to exploit gaps between criminal law and national security doctrine.

3.3.2 Threats to diaspora communities and regional spillover

The IRI's growing use of criminal intermediaries to target regime opponents abroad has intensified the threat landscape for Iranian diaspora communities. Dissidents who once believed in Western asylum protections now face a form of 'transnational repression' – a term describing how authoritarian regimes surveil, harass, threaten, and even physically harm exiles living in democratic states.[84] Iran's approach uniquely blends state intelligence, diplomatic cover, and state-linked criminal intermediaries to conduct such repression beyond its borders.

These operations increasingly target not only dissidents but also Israeli-linked institutions and individuals, using criminal intermediaries to execute arson, surveillance, and violence. These attacks are calculated gray zone operations: calibrated to intimidate, disrupt, and avoid attribution. These incidents are not merely isolated crimes – they are manifestations of hybrid statecraft that weaponize democratic openness. As such, they demand responses that combine domestic security with foreign policy foresight.

In this context, host countries risk becoming indirect arenas for regional conflict. Events in the Middle East – such as Iranian-Israeli tensions – can ripple out into Europe and North America via covert operations executed by criminal proxies. This underscores the need for foreign policy awareness to inform domestic security strategies. Governments that fail to anticipate such spillover effects may be caught off guard – not only by violent acts but by the diplomatic, legal, and social consequences they generate.

3.3.3 Law enforcement recognition and Intelligence consensus

Most democracies already criminalize threats and violence, but their legal tools are often insufficient against subtle, contracted, and cross-border intimidation. The real problem lies in identifying and prosecuting foreign-directed coercion spread across multiple jurisdictions.[85] Current frameworks often treat such incidents as isolated crimes, rather than components of a strategic campaign. This makes it essential to update legal and institutional responses so that foreign-directed harassment is recognized as a national security concern. Doing so would allow prosecutors and security services to build cumulative cases rather than isolated charges.

Growing international recognition of this threat has led to a more assertive response. In January 2024, the U.S. Department of the Treasury sanctioned Iranian narcotics trafficker Naji Ibrahim Sharifi Zindashti, identifying his group as a key actor in Iranian state-directed kidnappings and assassinations targeting dissidents across multiple countries.[86] In May 2024, Sweden's Security Service (Säpo[87]) declared publicly that the IRI was using Swedish criminal networks to carry out violent attacks, including thwarted operations against Israeli and Jewish targets.[88] Säpo's counterespionage chief, Daniel Stenling, stated that the service had established clear links between Iranian intelligence and domestic criminal gangs.[89]

In the UK, MI5 Director General Ken McCallum[90] revealed in 2024 that the UK had disrupted 20 Iranian-backed plots since 2022, emphasizing the regime's use of both high-level traffickers and low-level criminals. Meanwhile, in the United States, the Department of Justice confirmed that members of an Eastern European organized crime group were contracted by IRGC-linked operatives in a failed murder-for-hire scheme against a U.S.-based dissident.[91] Rafat Amirov and Polad Omarov, convicted in March 2025, had coordinated the plot using instructions from Iranian handlers.

These examples reflect a growing consensus in the literature: the use of criminal networks by states is not merely a law-enforcement challenge but a transnational security threat requiring integrated legal, diplomatic, and intelligence responses.[92] The fusion of criminal and state interests in extra-territorial violence – seen historically in Yugoslavia's UDBA[93] operations and

Russia's post-Soviet intelligence-crime nexus[94]—risks normalizing a new standard of clandestine competition.

These revelations confirm that Iran's criminal outsourcing is no longer a theoretical concern, but an empirically verified, transnational threat that spans continents and legal systems.

3.3.4 Reputational warfare and the future of outsourced coercion

As international scrutiny increases the risks associated with physical operations, Iran is likely to pivot toward more indirect forms of coercion. This strategic adaptation preserves the core logic of GZS: calibrating repression to remain below the threshold of decisive response. One emerging avenue is reputational coercion. That is targeting dissidents not through violence but through disinformation and defamation designed to discredit and delegitimize them. When assassination plots or physical intimidation become too risky due to enhanced vigilance or diplomatic costs, the regime may increasingly adopt narrative-based tactics; spreading rumors, manipulating media, and orchestrating scandals to isolate dissidents and fracture diaspora communities.

These tactics are already central to the playbooks of many authoritarian states where coordinated smear campaigns often involving fake news, staged scandals, and fabricated accusations, target critics to neutralize opposition and sow distrust.[95] The IRI is well-positioned to adopt and adapt these techniques to its global repression strategy. Repeated and viral messaging gives such falsehoods traction, forcing dissidents to expend energy defending themselves while eroding their credibility.

Such campaigns often blur the lines between moral, sexual, and criminal accusations. 'Honey traps', for example, can be staged not only for intelligence gathering or kidnappings, as the IRI has done,[96] but also to engineer public scandal. Even false claims of sexual misconduct or other criminal offences can irreparably damage reputations, especially when they tap into preexisting societal biases. Investigative journalist Omar Radi in Morocco and former Rwandan diplomat-turned-dissident Eugène Richard Gasana were both targeted with rape allegations in contexts widely viewed as politically charged; cases that underscore how sexual charges can be weaponized to silence dissent.[97] Such methods serve the same purpose as assassinations – neutralizing threats – only with different instruments.

Democratic states have also employed similar tactics. During the U.S. government's COINTELPRO operation (1950s–70s), the FBI used forged letters, planted media stories, and personal smears to isolate civil rights leaders and anti-war activists.[98] These strategies aimed not only to discredit individuals but to dismantle opposition movements from within. These historical parallel reveals that even democracies have recognized the utility of

reputational warfare – an insight authoritarian regimes now exploit with far fewer constraints.

The IRI's use of sexualized smear campaigns is already evident. In October 2022, the pro-regime Telegram channel 'Adl-e Ali' circulated photographs of Yasmin Pahlavi, wife of prominent opposition leader Crown Prince Reza Pahlavi, with a French man, framing the images as evidence of marital infidelity.[99] State-aligned outlets amplified the story, labeling it a 'moral scandal'. In some iterations, the narrative escalated into wholly invented allegations of divorce and mutual infidelity.[100]

The IRI's likely turn toward such tactics presents a serious challenge to Western law enforcement, which often prioritizes physical threats over reputational or psychological coercion. These forms of soft coercion operate in legal and evidentiary blind spots, making them harder to detect, prosecute, or even acknowledge as part of hostile foreign activity. As with hired violence, the ambiguity of authorship is a feature of this strategy. To counter them, democratic governments must invest in counter-disinformation infrastructure, promote digital literacy, and expand legal definitions to include cross-border narrative warfare as a national security concern. Intelligence and law enforcement agencies should also develop indicators and early warning systems for reputational attacks linked to foreign interference. Without such reforms, authoritarian regimes will continue to exploit legal gray zones – undermining dissent not through violence, but through story. In the age of hybrid repression, silencing voices no longer requires pulling a trigger; only crafting a lie.

4. Conclusion

This paper has reassessed the covert security doctrine of the Islamic Republic of Iran, showing how outsourced violence is not ad hoc, but a central, systematized element of Iran's coercive toolkit. The regime's use of state-linked criminal intermediaries to carry out assassinations and acts of repression abroad reflects a deliberate fusion of strategic imperatives and ideological motivations.

GZS helps explain this logic: Tehran relies on ambiguous, untraceable operations to project power, deter opposition, and suppress dissent while avoiding direct confrontation. These tactics allow Iran to advance its goals below the threshold of open conflict, making use of intermediaries who offer both local access and attributional cover.

Over time, the regime's campaigns – once conducted primarily through ideologically aligned proxies – have evolved into more flexible, transactional collaborations with organized crime. This historical shift, from revolutionary zeal to pragmatic outsourcing, reflects Tehran's adaptation to international countermeasures and operational limitations. The turn to criminal

intermediaries lowers visibility, exploits Western legal and institutional vulnerabilities, and extends Iran's coercive reach across Europe and North America.

Recent revelations and prosecutions confirm that this outsourcing is no longer peripheral. As this paper has shown, the evolution from ideological actors to criminal surrogates demands new approaches to both attribution and deterrence. Iran's extraterritorial violence is now a rational instrument of statecraft, deployed strategically under conditions of constraint. To counter this growing threat, policymakers must need to consider treating Iranian-backed assassinations not merely as isolated crimes but as sophisticated instruments of state-level coercion. An effective response will require integrated strategies combining intelligence sharing, legal reforms, and coordinated diplomatic pressure to close the gray zones that Iran so effectively exploits. By recognizing the connections between ideology, strategy, and illicit networks, democratic states stand a better chance of confronting and disrupting the Islamic Republic's machinery of transnational repression.

Notes

1. Iran Human Rights Documentation Center, "No safe haven".
2. Shokouhi, "تاییدی بر ادعای چرخش فریدون فرخزاد به سمت جمهوری اسلامی [A Confirmation of the Claim that Fereydoun Farrokhzad Turned Toward the Islamic Republic]."
3. Didban Iran, "گفت و گو با محسن رفیق دوست: از پرونده فاضل خداداد تا ماجرای قاچاق دختران ایرانی به کشورهای [Interview with Mohsen Rafiqdoost: From the Fazel Khodadad case to the trafficking of Iranian girls to Arab countries]."
4. AbdiMedia – Abdollah Abdi [@abdolah_abdi], "*O* □ #/ویژه/#انتشار_برای_نخستین_بار [X] [Exclusive/#PublishedForTheFirstTime/How the Islamic Republic's Assassination Budget in Europe Is Funded]."
5. Bank Saderat Iran (English translation: Iran Export Bank), founded in 1952, has several offices outside the country. Since 2006, it has been sanctioned by the United States for supporting terrorism.
6. Levitt, "Introducing the Iranian External Operations Interactive Map and Timeline."
7. Central Intelligence Agency, "A Consumer's Guide to Intelligence."
8. Morris et al., *Gaining Competitive Advantage*, 8.
9. Ibid., 8–12
10. Mazarr, "Mastering the Gray Zone"; and Jordan, "International Competition Below the Threshold of War," 1–24.
11. Mazarr, "Mastering the Gray Zone."
12. Brands, "Paradoxes of the Gray Zone."
13. Azad, Haider, and Sadiq, "Understanding Gray Zone Warfare," 81–104.
14. Rauta, "Toward a Typology of Non-State Actors in 'Hybrid Warfare'," 868–87.
15. Rabasa et al., *Counternetwork*; Eisenstadt, "Iran's Gray Zone Strategy"; and Mailey, "Iran´s Criminal Statecraft," 1–54.

16. Levitt, "Introducing the Iranian External Operations Interactive Map and Timeline"; Long, "Shadows of Power"; and Levitt, "Trends in Iranian External Assassination," 1–11.
17. e.g., Swedish Security Service, "Iran is Using Criminal Networks"; and Khoshnood, "The Role of the Qods," 4–33.
18. Jordan, "Threshold of War International Competition Below the Threshold of War," 1–24.
19. Khoshnood, "The Role of the Qods," 4–33.
20. Carment and Belo, "Gray-Zone Conflict Management," 21–41.
21. Eisenstadt, "Iran's Gray Zone Strategy."
22. Braw, "Countering Aggression," 62–75.
23. Morris et al., Gaining Competitive Advantage, 2,6.
24. Hoffman,"The Missing Element in Crafting National Strategy," 55–64
25. Tadjbakhsh, "International Relations Theory," 181; and Mashregh, "اپوزیسیون وطنی یا کوتولههای وابسته به رژیم صهیونیستی؟" [Domestic Opposition or Dwarfs Affiliated with the Zionist Regime?].
26. Byman, "Iran, Terrorism," 169–81
27. Khoshnood, "The Role of the Qods," 4–33; Levitt, "Iran's Deadly Diplomats," 10–5; and Wege, "Iranian Intelligence Organizations," 287–98
28. United Press International, "Shah's Nephew Assassinated."
29. Sayami, مستند تلویزیونی شرقی غمگین: دفتر سوم [Sad Eastern: Television Documentary, Volume Three]; and Iran Human Rights Documentation Center, "No safe haven.
30. United Press International. "Two Iranian Exiles."
31. Hicks, Schaus, and Matlaga, *Zone Defense*.
32. Braw, "Countering Aggression," 62–75.
33. *Bakhtiar v. Islamic Republic of Iran*, 571 F. Supp. 2d 27 (D.D.C. 2008).
34. Iran Human Rights Documentation Center, "Murder at Mykonos."
35. Becker and Wiedmann-Schmidt, "Drecksarbeit für die Mullahs"; Gozzi, "Iran may be Behind Attacks"; Swedish Security Service, "Iran is Using Criminal Networks"; DePrado and Zagaris, "International Human Rights," 89–92; Khoshnood, *Iran's Killing Machine*; and Levitt, "Trends in Iranian External Assassination," 1–11.
36. Becker and Wiedmann-Schmidt, "Drecksarbeit für die Mullahs"; Gozzi, "Iran may be Behind Attacks"; Swedish Security Service, "Iran is Using Criminal Networks"; and DePrado and Zagaris, "International Human Rights," 89–92.
37. The Qods Force is the extraterritorial arm of the IRGC.
38. Office of Public Affairs, "Two Eastern European."
39. U.S. Department of the Treasury, "Treasury Sanctions Five Individuals."
40. Eisenstadt, "Iran's Gray Zone Strategy"; Al-Jabassini, "From rebel leaders to Post-War Intermediaries," 656–77; and Karlén and Rauta, "Dealers and Brokers in Civil Wars."
41. Rauta, "Toward a Typology of non-State Actors in 'Hybrid Warfare'," 868–87.
42. e.g. Becker and Wiedmann-Schmidt, "Drecksarbeit für die Mullahs"; Gozzi, "Iran may be Behind Attacks"; Swedish Security Service, "Iran is Using Criminal Networks"; and DePrado and Zagaris, "International Human Rights," 89–92.
43. Europol,"Decoding the EU's Most Threatening."
44. Levitt, "Trends in Iranian External Assassination," 1–11; Eisenstadt, "Iran's Gray Zone Strategy"; Levitt, "Iran's Deadly Diplomats," 10–5; and Khoshnood, "The Role of the Qods," 4–33.

45. Levitt, "Iran's Deadly Diplomats," 10–5; Khoshnood, *Iran's Killing Machine*; and Al-Jabassini, "From rebel leaders to Post-War Intermediaries," 656–77.
46. Azad, Haider, and Sadiq, "Understanding Gray Zone Warfare," 81–104.
47. Ban, "Lopsided Security on the Korean Peninsula," 441–66.
48. Jordan, "International Competition Below the Threshold of War," 1–24.
49. Galeotti, "Gangsters at War," 1–58.
50. O'Neill, "Countering North Korean Cybercrime."
51. DePrado and Zagaris, "International Human Rights," 89–92; Office of Public Affairs, "Two Men Charged"; and Office of Public Affairs, "Two Eastern European."
52. Algemene Inlichtingen- en Veiligheidsdienst.
53. General Intelligence and Security Service of the Netherlands and National Coordinator for Counterterrorism and Security, "Crossing Borders."
54. U.S. Department of the Treasury, "The United States and United Kingdom Target."
55. Ibid.
56. Khoshnood, "ASMLA: An Empirical Exploration."
57. DePrado and Zagaris, "International Human Rights," 89–92.
58. DePrado and Zagaris, "International Human Rights," 89–92; and U.S. Department of the Treasury, "The United States and United Kingdom Target."
59. Levitt, "Introducing the Iranian External Operations Interactive Map and Timeline."
60. Becker and Wiedmann-Schmidt, "Drecksarbeit für die Mullahs."
61. Gozzi, "Iran May be Behind Attacks."
62. Iran Human Rights Documentation Center, "Murder at Mykonos"; Khoshnood, *Iran's Killing Machine;* Khoshnood and Khoshnood, "The Islamic Republic," 976–92; and Levitt, "Iran's Deadly Diplomats," 10–5.
63. Levitt, "Introducing the Iranian External Operations Interactive Map and Timeline."
64. Sayami, "مستند تلویزیونی شرقی غمگین: دفتر سوم [Sad Eastern: Television Documentary, Volume Three]."
65. Didban Iran, "گفت و گو با محسن رفیق دوست: از پرونده فاضل خداداد تا ماجرای قاچاق دختران ایرانی به کشورهای عربی [Interview with Mohsen Rafiqdoost: From the Fazel Khodadad case to the trafficking of Iranian girls to Arab countries]."
66. Normark, "How States use Non-State Actors."
67. Didban Iran, "گفت و گو با محسن رفیق دوست: از پرونده فاضل خداداد تا ماجرای قاچاق دختران ایرانی به کشورهای [Interview with Mohsen Rafiqdoost: From the Fazel Khodadad case to the Trafficking of Iranian girls to Arab countries]."
68. Khoshnood, "The Role of the Qods," 4–33; Katzman, *Iran's Foreign Policy;* Levitt, "Iran's Deadly Diplomats," 10–5; and Levitt, "Trends in Iranian External Assassination," 1–11.
69. Wehrey et al., *The Rise of the Pasdaran.*
70. Iran Human Rights Documentation Center. "No Safe Haven."
71. Argentine-Israeli Mutual Association.
72. Alberto Nisman was an Argentine prosecutor who led the investigation into the AMIA bombing. On January 19, 2015, he was found shot dead in his residence. His death remains an unsolved case.
73. Nisman and Burgos, "AMIA Case"; Khoshnood, "The Role of the Qods," 4–33.
74. Perliger and Palmieri, "Mapping Connections and Cooperation," 335–47.
75. Normark, "How States use Non-State Actors."

76. Long, "Shadows of Power."
77. Khoshnood and Khoshnood, "The Islamic Republic," 976–92.
78. Belli et al., "Exploring the Crime," 263–81; and Vianna de Azevedo, *The Nexus The Nexus Between Transnational Organized Crime and Terrorism*.
79. Shaw, "Beyond Necessity," 582–604.
80. Belli et al., "Exploring the Crime," 263–81.
81. Normark, "How States Use Non-State Actors."
82. Braw, "Countering Aggression," 62–75; and Notaker, "In the Blind Spot."
83. Khoshnood and Khoshnood, "The Islamic Republic," 976–92; and Levitt, "Iran's Deadly Diplomats," 10–5.
84. Schenkkan and Linzer, *Transnational Repression*.
85. Ibid.
86. U.S. Department of the Treasury, "The United States and United Kingdom target."
87. Säkerhetspolisen.
88. Swedish Security Service, "Iran is using Criminal Networks."
89. Olsen, "Stockholm Accuses Iran."
90. McCallum, "Director General Ken McCallum."
91. Office of Public Affairs, "Two Eastern European."
92. Rabasa et al., *Counternetwork*; Lennox, "Threat Convergence: Transnational Organized Crime."
93. The UDBA, an acronym for its Serbian name Uprava državne bezbednosti, was Yugoslavia's Directorate for State Security, established in 1946 and dissolved in 1991.
94. Galeotti, "Gangsters at War," 1–58; and Nielsen, "Yugoslavia and Political Assassinations"
95. e.g., Andrew and Mitrokhin, *The Sword and the Shield*, 40, 319; Bonnie, "Political Abuse," 136–44; Gel'man, "The Politics of Fear," 6–26; Han, "Manufacturing Consent," 105–34; King, Pan, and Roberts, "How the Chinese Government," 484–501; Munro, "Judicial Psychiatry," 1–128; and Pearce, "Democratizing Kompromat," 1158–74.
96. DePrado and Zagaris, "International Human Rights," 89–92; and The Economist, "Go Hang"
97. Human Rights Watch, "Morocco: Journalist in Prison"; abd Mureithi and Zalan, "Rwanda Fed False Intelligence."
98. Day and Whitehorn, "Human Rights in the United States."
99. Mashregh, "جنجال حضور مرد فرانسوی کنار همسر رضا پهلوی+ عکس [The scandal over the presence of a French man next to Reza Pahlavi's wife + photo]"; and Young Journalists Club, "واکنش کاربران به حضور مرد فرانسوی کنار همسر رضا پهلوی [Users' reaction to the presence of a French man next to Reza Pahlavi's wife]."
100. Mashregh, "تصاویر لورفته شاهزاده ربع پهلوی با معشوقه جدید [Leaked photos of Prince Pahlavi with a new lover]."

Acknowledgments

The author acknowledges the use of ChatGPT (GPT-4/5, OpenAI, March 2024 version) and Microsoft Copilot (version 1.25023.101.0, Microsoft 365) during the preparation of this manuscript. These tools were used to support language refinement, structural suggestions, editing support, and synthesis of author-provided content, with the

purpose of enhancing clarity, coherence, and readability—particularly as the author is not a native English speaker. Neither tool was used to generate original research ideas or theoretical framing. All outputs were rigorously and critically reviewed, edited, and verified by the author, who takes full responsibility for the final content of the manuscript.

This use complies with the Taylor & Francis AI policy on the responsible use of generative AI in scholarly publishing: https://taylorandfrancis.com/our-policies/ai-policy/. It is also consistent with Lund University's AI policy, which permits the use of tools such as Microsoft Copilot by employees: https://www.education.lu.se/en/article/lu-employees-can-now-use-ai-assistant-copilot-previously-known-bing-chat-free.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Ardavan M. Khoshnood is an associate professor and senior lecturer of emergency medicine at Lund University in Sweden and a criminologist who focuses on offender profiling and violent crimes, including terrorism. He holds a degree in Political Science from Malmö University, a degree in Intelligence Analysis from Lund University, and a degree in Police Work from Umeå University. He Specializes in Iranian foreign policy, the Islamic Revolutionary Guard Corps and the Ministry of Intelligence.

ORCID

Ardavan M. Khoshnood http://orcid.org/0000-0002-3142-4119

Bibliography

AbdiMedia - Abdollah Abdi. "O #ویژه/#انتشاربرای‌نخستین_بار/بودجه ترورهای جمهوری اسلامی در اروپا چگونه تامین میشد." [Exclusive/#PublishedForTheFirstTime/How the Islamic Republic's Assassination Budget in Europe Is Funded]." *X*. March 9, 2025. https://x.com/abdolah_abdi/status/1898858837769159116.

Al-Jabassini, Abdullah. "From Rebel Leaders to Post-War Intermediaries: Evidence from Southern Syria." *Small Wars and Insurgencies* 35, no. 4 (2024): 656–677. doi:10.1080/09592318.2024.2312626.

Andrew, Christopher, and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 2000.

Azad, Tahir Mahmood, Muhammad Waqas Haider, and Muhammad Sadiq. "Understanding Gray Zone Warfare from Multiple Perspectives." *World Affairs* 186, no. 1 (2023): 81–104. doi:10.1177/00438200221141101.

Bakhtiar v. Islamic Republic of Iran, 571 F. Supp. 2d 27 (D.D.C. 2008)

Ban, K. J. "Lopsided Security on the Korean Peninsula: North Korea's Gray Zone Evolution from Balance of Insecurity to Imbalance of Terror." *Asian Survey* 62, no. 3 (2022): 441–466. doi:10.1525/as.2021.1434294.

Becker, S., and W. Wiedmann-Schmidt. "Drecksarbeit Für Die Mullahs." *Der Spiegel* 37 (2024): 36–38.

Belli, R., J. D. Freilich, S. M. Chermak, and K. A. Boyd. "Exploring the Crime–Terror Nexus in the United States: A Social Network Analysis of a Hezbollah Network Involved in Trade Diversion." *Dynamics of Asymmetric Conflict* 8, no. 3 (2015): 263–281. doi:10.1080/17467586.2015.1104420.

Bonnie, R. J. "Political Abuse of Psychiatry in the Soviet Union and in China: Complexities and Controversies." *The Journal of the American Academy of Psychiatry and the Law* 30 (2002): 136–144. doi:10.2139/ssrn.1760001.

Brands, H. "Paradoxes of the Gray Zone." 2016. Accessed June 5, 2025. https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Braw, E. "Countering Aggression in the Gray Zone." *Prism* 9 (2021): 62–75.

Byman, D. "Iran, Terrorism, and Weapons of Mass Destruction." *Studies in Conflict and Terrorism* 31, no. 3 (2008): 169–181. doi:10.1080/10576100701878424.

Carment, D., and D. Belo. "Gray-Zone Conflict Management: Theory Evidence, and Challenges." *The Air Force Journal of European, Middle Eastern and African Affairs* 2 (2020): 21–41. https://airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zoneconflict-%20management-theory-evidence-and-challenges/.

Central Intelligence Agency. *A Consumer's Guide to Intelligence*. Washington DC: Office of Public Affairs, Central Intelligence Agency, 1999.

Day, S., and L. Whitehorn. "Human Rights in the United States: The Unfinished Story of Political Prisoners and COINTELPRO." *New Political Science* 23, no. 2 (2001): 285–297. doi:10.1080/07393140120056009.

DePrado, J., and B. Zagaris. "International Human Rights." *International Enforcement Law Reporter* 40 (2024): 89–92.

Didban Iran. گفت و گو با محسن رفیق دوست: از پرونده فاضل خداداد تا ماجرای قاچاق دختران ایرانی به کشورهای عربی. [Interview with Mohsen Rafiqdoost: From the Fazel Khodadad case to the trafficking of Iranian girls to Arab countries.] *YouTube*. 2025. https://youtu.be/aWfDgAwI9xU?si=BfSUfDqyfxH0sh0H.

The Economist. "Go Hang." *Economist*, 2020: 89.

Eisenstadt, M. "Iran's Gray Zone Strategy." *Prism* 9 (2021): 76–97.

Europol. "Decoding the EU's Most Threatening Criminal Networks." 2024. https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks.

Galeotti, M. "Gangsters at War: Russia´s Use of Organized Crime as an Instrument of Statecraft." 2024. https://globalinitiative.net/analysis/gangsters-at-war-russias-use-of-organized-crime-as-an-instrument-of-statecraft/.

Gel'man, V. "The Politics of Fear." *Russian Politics & Law* 53, no. 5–6 (2015): 6–26. doi:10.1080/10611940.2015.1146058.

General Intelligence and Security Service of the Netherlands and National Coordinator for Counterterrorism and Security. "Crossing Borders: State-Sponsored Interference in Diaspora Communities in the Netherlands"." 2024. Accessed April 9, 2025. https://english.nctv.nl/binaries/nctv-en/documenten/publications/2025/03/24/phenomenon-analysis-crossing-borders/Crossing+Borders+AIVD-NCTV.pdf .

Gharebaghi, M. "ماهیت صهیونیستی مخالفان جمهوری اسلامی ایران." [The Zionist Nature of the Opponents of the Islamic Republic of Iran]." *Javan Online*. 2023. Accessed April 9, 2025. https://www.javanonline.ir/0051pG .

Gozzi, L. "Iran May Be Behind Attacks on Israeli Embassies, Sweden Says." *BBC*. 2024. Accessed April 9, 2025. https://www.bbc.com/news/articles/cvglk3md4e3o.

Han, Rongbin. "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army'." *Journal of Current Chinese Affairs* 44, no. 2 (2015): 105–134.

Hicks, Kathleen H., John Schaus, and Michael Matlaga. *Zone Defense: Countering Competition in the Space Between War and Peace*. Washington D.C.: Center for Strategic and International Studies, 2018.

Hoffman, Frank G. "The Missing Element in Crafting National Strategy: A Theory of Success." *Joint Force Quarterly* 97 (2020): 55–64. doi:10.1177/186810261504400205.

Human Rights Watch. "Morocco: Journalist in Prison After Unfair Trial." *Human Rights Watch*. Accessed April 10, 2025. https://www.hrw.org/news/2021/11/25/morocco-journalist-prison-after-unfair-trial .

Iran Human Rights Documentation Center. "No Safe Haven: Iran's Global Assassination Campaign." 2008. https://iranhrdc.org/no-safe-haven-irans-global-assassination-campaign/.

Iran Human Rights Documentation Center. "Murder at Mykonos: Anatomy of a Political Assassination." 2011. https://iranhrdc.org/murder-at-mykonos-anatomy-of-a-political-assassination/.

Jordan, Javier. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict." *Journal of Strategic Studies* 14 (2020): 1–24. 10.5038/1944-0472.14.1.1836.

Katzman, Kenneth. "*Iran's Foreign Policy*." CRS Report No. R44017. Congressional Research Service. 2016.

Khoshnood, Ardavan *Iran's Killing Machine: Political Assassinations by the Islamic Regime*. Ramat Gan: Mideast Security and Policy Studies No. 185. Begin-Sadat Center for Strategic Studies, 2020a.

Khoshnood, Ardavan "The Role of the Qods Force in the Foreign Policy of the Islamic Republic of Iran." *Central European Journal of International & Security Studies* 14, no. 3 (2020b): 4–33. doi:10.51870/CEJISS.A140301.

Khoshnood, Ardavan M., and Arvin Khoshnood. "The Islamic Republic of Iran's Use of Diplomats in Its Intelligence and Terrorist Operations Against Dissidents: The Case of Assadollah Assadi." *International Journal of Intelligence & Counterintelligence* 37, no. 3 (2024): 976–992. doi:10.1080/08850607.2023.2295205.

Khoshnood, Arvin. "ASMLA: An Empirical Exploration of an Ethno-Nationalist Terrorist Organization." Mideast Security and Policy Studies No. 193. Begin-Sadat Center for Strategic Studies. 2021. http://www.jstor.org/stable/resrep34340.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *The American Political Science Review* 111, no. 3 (2017): 484–501. doi:10.1017/S0003055417000144.

Lennox, Patrick. "Threat Convergence: Transnational Organized Crime and Canadian State Adaptation in the New International Security Context." In *Canada Among Nations 2023: Twenty-First Century National Security*, edited by Norman Hillmer, Philippe Lagassé, and Vincent Rigby, 319–338. Cham: Palgrave Macmillan.

Levitt, Matthew. "Iran's Deadly Diplomats." *CTC Sentinel* 11 (2018): 10–15.

Levitt, Matthew. "Trends in Iranian External Assassination, Surveillance, and Abduction Plots." *CTC Sentinel* 15 (2022): 1–11.

Levitt, Matthew. *Introducing the Iranian External Operations Interactive Map and Timeline*. Washington D.C.: The Washington Institute for Near East Policy, 2024.

Long, Magda. "Shadows of Power Beneath the Threshold: Where Covert Action, Organized Crime and Irregular Warfare Converge." *Intelligence and National Security* 40, no. 1 (2025): 87–113. doi:10.1080/02684527.2024.2417454.

Mailey, J. R. "Iran's Criminal Statecraft: How Tehran Weaponizes Illicit Markets." 2024. https://globalinitiative.net/analysis/irans-criminal-statecraft-how-teheran-weaponizes-illicit-markets/ .

Mashregh. ""اپوزیسیون وطنی یا کوتولههای وابسته به رژیم صهیونیستی؟." [Domestic Opposition or Dwarfs Affiliated with the Zionist Regime?]." *Mashregh News*. Accessed April 9, 2025a. https://mshrgh.ir/1474700.

Mashregh. ""جنجال حضور مرد فرانسوی کنار همسر رضا پهلوی+ عکس" [The Scandal Over the Presence of a French Man Next to Reza Pahlavi's Wife + Photo]." *Mashregh News*. Accesed August 8, 2025b. https://mshrgh.ir/1460215.

Mashregh. ""تصاویر لورفته شاهزاده ربع پهلوی با معشوقه جدید" [Leaked photos of Prince Pahlavi with a new lover]." *Mashregh News*. August 8, 2025c. https://mshrgh.ir/1466916.

Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Pennsylvania: US Army War College Press, 2015.

McCallum, Ken. "Director General Ken McCallum Gives Latest Threat Update." *MI5*. Accessed April 7, 2025. https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stéphanie Pézard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone*. Santa Monica: RAND Corporation, 2019.

Munro, Robin. "Judicial Psychiatry in China and Its Political Abuses." *Columbia Journal of Asian Law* 14, no. 1 (2000): 1–128. doi:10.52214/cjal.v14i1.13664.

Mureithi, Carlos, and Kira Zalan. "Rwanda Fed False Intelligence to U.S. and INTERPOL as It Pursued Political Dissidents Abroad." *Organized Crime and Corruption Reporting Project*. Accessed April 10, 2025. https://www.occrp.org/en/investigation/rwanda-fed-false-intelligence-to-us-and-interpol-as-it-pursued-political-dissidents-abroad .

Nielsen, Christian Axboe. *Yugoslavia and Political Assassinations: The History and Legacy of Tito's Campaign Against the Emigrés*. London: Bloomsbury Publishing, 2022.

Nisman, Alberto, and Marcelo M. Burgos. "AMIA Case." Office of Criminal Investigations. Investigations Unit of the Office of the Attorney General, 2006.

Normark, Magnus. "How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks." *Hybrid Coe Strategic Analysis*, 2019, Hybrid CoE.

Notaker, Hallvard. "In the Blind Spot: Influence Operations and Sub-threshold Situational Awareness in Norway." *Journal of Strategic Studies* 46, no. 3 (2023): 595–623. doi:10.1080/01402390.2022.2039634.

Office of Public Affairs. "Two Eastern European Organized Crime Leaders Convicted of Murder for Hire Targeting U.S.-Based Journalist on Behalf of Iranian Government." *United States Department of Justice*. Accessed April 7, 2025a. https://www.justice.gov/opa/pr/two-eastern-european-organized-crime-leaders-convicted-murder-hire-targeting-us-based.

Office of Public Affairs. "Two Men Charged in Alleged Plot to Assassinate Saudi Arabian Ambassador to the United States." *United States Department of Justice*. Accessed April 7, 2025b. https://www.justice.gov/archives/opa/pr/two-men-charged-alleged-plot-assassinate-saudi-arabian-ambassador-united-states.

Olsen, J. M. "Stockholm Accuses Iran of Using Criminals in Sweden to Target Israel or Jewish Interests." *AP*. Accessed April 7, 2025. https://apnews.com/article/sweden-iran-israel-criminal-gangs-proxy-d50a17efab629a585e281854d3e11407.

O'Neill, A. "Countering North Korean Cybercrime and Its Enablers." *Lawfare*. 2024. Accessed August 7, 2025. https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers.

Paul, T. V. "Soft Balancing in the Age of U.S. Primacy." *International Security* 30, no. 1 (2005): 46–71. doi:10.1162/0162288054894652.

Pearce, K. E. "Democratizing Kompromat: The Affordances of Social Media for State-Sponsored Harassment." *Information Communication & Society* 18, no. 10 (2015): 1158–1174. doi:10.1080/1369118X.2015.1021705.

Perliger, A., and M. Palmieri. "Mapping Connections and Cooperation Between Terrorist and Criminal Entities." *Studies in Conflict and Terrorism* 45, no. 5–6 (2022): 335–347. doi:10.1080/1057610X.2019.1678874.

Rabasa, Angel, Christopher M. Schnaubelt, Peter Chalk, Douglas Farah, Gregory Midgette, and Howard J. Shatz. *Counternetwork: Countering the Expansion of Transnational Criminal Networks*. Santa Monica: RAND Corporation, 2017.

Rauta, V. "Toward a Typology of Non-State Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate, and Affiliated Forces." *Cambridge Review of International Affairs* 33, no. 6 (2019): 868–887. doi:10.1080/09557571.2019.1656600.

Sayami, S., and H. Asgari. "مستند تلویزیونی شرقی غمگین: دفتر سوم." [Sad Eastern: Television Documentary, Volume Three]." *Radio Farda*. 2020. https://youtu.be/VLedFcuiMvM?si=hf-r3-AyWDYKsT25.

Schenkkan, Nate, and Isabel Linzer. *Transnational Repression*. Washington D.C.: Freedom House, 2021.

Shaw, D. O. "Beyond Necessity: Hezbollah and the Intersection of State-Sponsored Terrorism with Organised Crime." *Critical Studies on Terrorism* 12, no. 4 (2019): 582–604. doi:10.1080/17539153.2019.1592074.

Shokouhi, A. "تاییدی بر ادعای چرخش فریدون فرخزاد به سمت جمهوری اسلامی." [A Confirmation of the Claim That Fereydoun Farrokhzad Turned Toward the Islamic Republic]." *Didar News*. Accessed July 31, 2025. https://www.didarnews.ir/fa/news/11944/%D8%AA%D8%A7%DB%8C%DB%8C%D8%AF%DB%8C-%D8%A8%D8%B1-%D8%A7%D8%AF%D8%B9%D8%A7%DB%8C-%DA%86%D8%B1%D8%AE%D8%B4-%D9%81%D8%B1%DB%8C%D8%AF%D9%88%D9%86-%D9%81%D8%B1%D8%AE%D8%B2%D8%A7%D8%AF-%D8%A8%D9%87-%D8%B3%D9%85%D8%AA-%D8%AC%D9%85%D9%87%D9%88%D8%B1%DB%8C-%D8%A7%D8%B3%D9%84%D8%A7%D9%85%DB%8C.

Swedish Security Service. "Iran Is Using Criminal Networks in Sweden." *Swedish Security Service*. Accessed April 5, 2024. https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/news/news/2024-05-30-iran-is-using-criminal-networks-in-sweden.html.

Tadjbakhsh, Shahrbanou. "International Relations Theory and the Islamic Worldview." In *Non-Western International Relations Theory: Perspectives on and Beyond Asia*, edited by Amitav Acharya and Barry Buzan, 174–196. London: Routledge, 2010.

United Press International. "Two Iranian Exiles Are Assassinated in Paris." *Lodi News-Sentinel*, 1979.

United Press International. "Shah's Nephew Assassinated by 'Death Squad'." *Middlesboro Daily News*, 1984.

U.S. Department of the Treasury. "Treasury Sanctions Five Individuals Tied to Iranian Plot to Assassinate the Saudi Arabian Ambassador to the United States." *United States Department of the Treasury*. Accessed April 7, 2025b. https://home.treasury.gov/news/press-releases/tg1320.

U.S. Department of the Treasury. "The United States and United Kingdom Target Iranian Transnational Assassinations Network." *United States Department of the Treasury*. Accessed April 7, 2025a. https://home.treasury.gov/news/press-releases/jy2052.

Vianna de Azevedo, C. *The Nexus Between Transnational Organized Crime and Terrorism in Latin America*. Torino: United Nations Interregional Crime and Justice Research Institute, 2024.

Wege, Carl A. "Iranian Intelligence Organizations." *International Journal of Intelligence & Counterintelligence* 10, no. 3 (1997): 287–298. doi:10.1080/08850609708435351.

Wehrey, Frederic, Jerrold D. Green, Brian Nichiporuk, Alireza Nader, and Lydia Hansell. *The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps*. Santa Monica: RAND Corporation, 2008.

Young Journalists Club. "واکنش کاربران به حضور مرد فرانسوی کنار همسر رضا پهلوی" [Users' Reaction to the Presence of a French Man Next to Reza Pahlavi's Wife]." *Young Journalists Club*. Accessed August 8, 2025. https://www.yjc.ir/00Z2EF.