A Growing Security Threat: Iranian Intelligence Operations in Scandinavia (Part Two: Sweden)

Khoshnood, Arvin; Norell, Magnus; Khoshnood, Ardavan M.

Published in:
Middle East Quarterly

2025

Document Version:
Publisher's PDF, also known as Version of record

A Growing Security Threat: Iranian Intelligence Operations in Scandinavia (Part Two: Sweden)

By: Arvin Khoshnood, Magnus Norell, Ardavan M. Khoshnood

Note: This is the second part of a two-part article on Iranian intelligence operations in Scandinavia. Part One, which appeared in the journal's Summer 2025 issue, focused on the threat in Denmark and Norway. Part Two addresses the same topic in Sweden.

Introduction: Iranian Intelligence Operations in Sweden

In its 2023–2024 security assessment, the Swedish Security Service (*Säkerhetspolisen*, or Säpo) singled out the Islamic Republic of Iran (IRI) as a major national threat.[1] Säpo noted that the IRI's intelligence services routinely engaged in espionage to circumvent international sanctions and obtain advanced technology and expertise from Swedish research institutions and industries. Although no specific sectors were named, Iran—alongside Russia and China—was cited as a state seeking to develop high-tech capabilities in defiance of export controls. Beyond its pursuit of strategically sensitive or sanctioned technologies, the IRI was implicated in assassination plots on Swedish soil that targeted Iranian dissidents and citizens of hostile states. Tehran relied on proxies to conduct intelligence gathering and terrorist activities, with cyber espionage playing a key role in tracking and monitoring dissidents. The Iranian regime also mounted influence campaigns aimed at spreading disinformation and influencing policymakers.

[1] https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf.

The Assassination and Surveillance of Dissidents

The IRI has a long history of extraterritorial repression in Sweden. Its operations against Iranian dissidents and critics include surveillance, intimidation, cyber operations, and assassination. Abroad, the regime targets enemies through both diplomatic channels and covert intelligence methods. Over the years, Sweden expelled multiple IRI diplomats for espionage against Iranian dissidents. Espionage, however, is only one of several tools the regime uses to crack down on opponents;[2] lethal violence is another. In the early 1990s, for example, regime agents carried out an assassination operation that killed two exiled Iranians, while a third target survived.[3] Assassination remains a key instrument in the IRI's toolkit for eliminating opposition figures in Sweden and worldwide.

The Iranian regime's cyber operations further strengthen its repressive activities. In 2020, IRI hackers developed a fraudulent mobile application, falsely claiming affiliation with the Swedish Transport Agency (*Trafikverket*).[4] Marketed to Farsi speakers as a study aid for the Swedish driving license, the app—trafikverket.apk—was embedded with malicious spyware that allowed Iranian intelligence to access and control infected devices remotely. Once installed, the malware recorded phone calls, harvested passwords, extracted images, and tracked users' browsing history. The collected data was then transmitted via an encrypted server in France to Iran. Thousands of users are believed to have unknowingly downloaded the app, effectively turning their phones into surveillance tools. This operation illustrates the IRI's ongoing efforts to monitor and control Iranian exiles in Sweden.

---

[2] https://www.svd.se/a/b554ea7d-cdee-3302-9ed7-cf632da3c6ba/iran-utvisade-svensk-diplomat;https://www.sverigesradio.se/artikel/uppgifter-diplomat-pekades-ut-som-iransk-underrattelseofficer-av-sapo.

[3] https://www.gp.se/nyheter/sverige/unikt-atal-diktatur-bestallde-mord.31e7f4c3-b25c-48c6-a311-aebd46152a9b

[4] https://www.svt.se/nyheter/inrikes/iransk-spionapp-har-stulit-information-om-svenskar-under-trafikverkets-tackmantel.

The Islamic Republic's Stockholm embassy plays a central role in Tehran's campaign of repression against regime opponents. In November 2022, amid nationwide protests in Iran following Mahsa Amini's murder, an Iranian activist in Sweden received a threatening phone call from the Iranian embassy. Its purpose was to deter him from organizing demonstrations, including protests outside the embassy. The Swedish newspaper Göteborgs-Posten later confirmed that the call had originated from within the embassy.[5]

The regime has also used legal mechanisms to silence dissidents and critics in Sweden. In 2022, a Swedish publication ran an op-ed by Ardavan Khoshnood calling for the closure of the IRI's embassy due to its involvementin espionage and terrorism. In response, the embassy filed a complaint with the Swedish Media Ombudsman, alleging that Khoshnood's article was baseless and defamatory. The Ombudsman dismissed the complaint, and the Media Ethics Council subsequently upheld the decision.[6]

These actions align with the IRI's broader geopolitical strategy of neutralizing opposition figures abroad, suppressing anti-regime activism, and molding political opinion in Western countries. Sweden, home to a large Iranian diaspora, remains a key target of the regime's extraterritorial repression.

The Assassination Plot Against Swedish Jews

In April 2021, an Iranian couple that entered Sweden under false identities six years earlier (in 2015) was arrested. After years of living seemingly normal lives, the IRI activated them for an intelligence operation.[7] In early 2021, they were directed to map Swedish Jews as potential assassination targets. This case illustrates the IRI's use ofsleeper agents—individuals who remain dormant for extended periods before being mobilized for covert operations.Because such cases are difficult to detect, the discovery of this couple was particularly significant.

Despite serious security implications, the couple was deported without legal

---

[5] https://www.gp.se/nyheter/goteborg/ata-postade-pa-instagram-da-ringde-irans-ambassad-kommer-sta-dig-dyrt.59ca85de-fae5-4e67-a168- 29475a21cc3d

[6] https://ardavan.se/the-regime-in-iran-has-reported-me/

[7] https://www.svt.se/nyheter/inrikes/incidenter-kopplade-till-israels-ambassader-detta-vet-vi

action. The ability of agents to infiltrate Sweden under false identities highlights critical vulnerabilities in the country's screening and immigration system, especially during periods of high migration. The Islamic Republic's substantial investment in a long-term intelligence operation in Sweden—a country often considered peripheral to global security—underscores its strategic interest in Scandinavia as a platform to advance broader geopolitical objectives.

The targeting of Jewish citizens is especially alarming given the sharp rise in antisemitic attacks in Sweden following Hamas's October 7, 2023, terrorist assault on Israel. The Islamic Republic's antisemitism is explicit and deeply rooted in its ideological doctrine. Its leadership has repeatedly called for the destruction of the State of Israel and the targeting of Jewish communities worldwide. The IRI's assassination plots against Swedish Jews represent a logical extension of its broader geopolitical strategy, which includes supporting anti-Israel militias, funding terrorist proxies, and orchestrating intelligence operations against Jewish and Israeli interests in the West.

Attacks on Israeli Interests

In 2024, a series of attacks on the Israeli embassy in Stockholm raised serious concerns about possible collaboration between Swedish criminal networks and Iranian intelligence. In January, Swedish police neutralized an explosive device found outside the embassy. In May, gunfire near the embassy led to the arrest of a 14-year-old male suspect. Additional shots were fired at the embassy in October, further heightening security concerns.

Israeli intelligence identified the Foxtrot network—a Swedish criminal organization led by Rawa Majid—as responsible for several of these incidents on behalf of the Islamic Republic.[8] Majid, also known as the "Kurdish Fox," is currently based in Iran and has reportedly established ties with Iranian intelligence services. The same network was implicated in an earlier attack on the Israeli embassy in Copenhagen (see Part One in the journal's previous issue). These incidents are consistent with the Islamic Republic's broader strategy of targeting Israeli interests worldwide through proxies and criminal networks. In this way, the regime can extend its

[8] https://www.svt.se/nyheter/inrikes/incidenter-kopplade-till-israels-ambassader-detta-vet-vi

reach while maintaining plausible deniability.

Security-Threatening Activities Through Mosques

In February 2025, Imam Mohsen Hakimollahi of the Imam Ali Islamic Center was deported from Sweden after Säpo determined that the center's mosque had been engaged in activities that threatened Iranian dissidents and undermined Swedish national security. According to Säpo, the center's leadership was aware of these activities.[9] The Imam Ali Islamic Center, located in Järfälla outside Stockholm, is the largest Shiite religious institution in the Nordic region and oversees the Imam Ali Mosque. Hakimollahi also served as vice chairman of the Islamic Shia Associations in Sweden (ISS), an umbrella organization representing Shiite associations nationwide. Several of these ISS-affiliated groups receive state funding, raising concerns that the IRI exploits these networks through its close ties to both Hakimollahi and ISS.

Hakimollahi's deportation came six months after German authorities shut down the Imam Ali Mosque in Hamburg, which was directly linked to the Iranian regime through Hamburg's Islamic Center. German authorities established that the mosque was raising funds for Hezbollah and disseminating Iranian regime propaganda.[10] The case in Järfälla highlights how the IRI leverages religious institutions across Europe to conduct intelligence operations, advance its geopolitical agenda, and threaten both exiled dissidents and the security of host nations.

Encouraging Terrorism Through SMS

During the summer of 2023, Sweden faced a highly sensitive political climate. Its NATO application was stalled due to opposition from Turkey and Hungary; at the same time, the country felt increasingly vulnerable to Russian aggression. Compounding these tensions, a series of Quran burnings in Sweden sparked international controversy.[11]

---

9 https://www.sverigesradio.se/artikel/sapo-iran-anvander-moske-i-stockholm-for-underrattelsearbete.

10 https://www.welt.de/regionales/hamburg/article241958041/Islamismus-Stellvertretender-Leiter-des-Islamischen-Zentrums-Hamburg-kommt-Abschiebung-zuvor.html; https://www.sverigesradio.se/artikel/tysk-polis-gjorde-razzia-mot-moske-i-hamburg.

11 https://www.dn.se/sverige/hemliga-angreppet-mot-sverige-under-koranbranningarna/;https://www.aftonbladet.se/nyheter/a/8q92eA/iran-utforde-operation-mot-sverige.

Domestically, the incidents further deepened societal polarization: some advocated for legal restrictions while others defended these acts on grounds of freedom of speech.

In the midst of this turbulent period, the Islamic Revolutionary Guard Corps (IRGC) launched a cyber operation against Sweden. On August 1, 2023, an Iranian cyber group hacked into a Swedish SMS service, sending nearly 15,000 messages to recipients, urging them to seek revenge against those responsible for the Quran burnings.[12] The attack fueled unrest and deepened social divisions, exacerbating both Sweden's internal security challenges and its already delicate relationship with Turkey. Although police and prosecutors identified the IRGC as the perpetrator, the case was ultimately closed because the attackers were based in Iran and therefore beyond the reach of Swedish law enforcement.

The consequences of this operation extended beyond 2023. On January 30, 2025, Salwan Momika, a key figure in the Quran burnings in Sweden, was shot dead in his home in Södertälje. While the investigation remains ongoing, a connection between the IRGC's incitement campaign and subsequent acts of violence cannot be ruled out.[13] The SMS attack, coupled with the IRI's broader efforts to spread anti-Swedish discourse, helped create an environment that emboldened violent actors. Iran's Supreme Leader, Ali Khamenei, declared on X (formerly Twitter) that those who had burned the Quran deserved capital punishment, thereby, underscoring the regime's hostility toward Sweden.[14]

The Iranian regime's interference in Sweden during this period was deliberate and served two key geopolitical objectives. First, the regime sought to position itself as the leader of the Muslim world by portraying itself as the defender of Islam, weaponizing the Quran burnings to mobilize Islamic sentiment against Sweden and the West. Second, the regime sought to undermine Sweden's

---

[12] https://www.dn.se/sverige/hemliga-angreppet-mot-sverige-under-koranbranningarna/;https://www.aftonbladet.se/nyheter/a/8q92eA/iran-utforde-operation-mot-sverige; and https://www.aklagare.se/nyheter-press/pressmeddelanden/2024/september/grovt-dataintrang-utfort-av-iran/; https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-09-24-dataintrang-bakom-paverkanskampanj.html.

[13] https://www.folkbladet.se/debatt/artikel/experten-de-kraver-sharialagar-i-sverige/jvqmmwer?s=08

[14] https://www.altinget.se/artikel/islamiska-regimen-i-iran-hetsar-mot-sverige.

NATO accession by aligning with Russia's interests. It pursued this goal by stoking domestic instability and heightening tensions with Turkey's President Recep Tayyip Erdoğan, who initially opposed the country's membership in the alliance.

Influence Operations Through Academia and Think Tanks

Recent investigations have uncovered troubling instances of IRI infiltration of Swedish academic and policy institutions. One notable case involves Rouzbeh Parsi, director of the Middle East program at the Swedish Institute of International Affairs (UI). Leaked emails reported by Swedish TV4 News indicated that Parsi participated in the Iran Experts Initiative (IEI), a network coordinated by the Iranian Foreign Ministry to influence Western perceptions of the regime.[15] In the emails, a senior Iranian diplomat referred to Parsi and his colleagues as "our friends." Parsi denied acting as an influence agent, asserting his involvement was purely academic. Publicly, Jakob Hallgren, director of UI, expressed continued confidence in Parsi; however, he launched an internal investigation, responding to concerns raised by Sweden's Ministry for Foreign Affairs.

In another incident, a former employee of the Iranian Ministry of Intelligence and Security (Vezarat-e Ettela'at va Amniyat-e Keshvar, or VAJA) was awarded a Ph.D. from Lund University in February 2025.[16] The integration of thisformer intelligence analyst into Swedish academia has sparked serious concerns regarding the Islamic Republic's use of academic institutions to advance its strategic objectives.

Yet another case concerned a Ph.D. student at the Royal Institute of Technology (KTH) in Stockholm who was found to have collaborated closely with the regime's Stockholm embassy. Among the student's primary contacts was Hamid Mollavali, a diplomat suspected of espionage by Säpo.[17] These connections, which led to the student's expulsion in spring

---

[15] https://www.tv4.se/artikel/4f72OQx4G6N0Mk0NTxiX8Y/iranexperten-rouzbeh-parsi-kopplas-till-paverkansnaetverk

[16] https://www.expressen.se/nyheter/sverige/jobbade-for-irans-underrattelsetjanst-fick-tjanst-pa-lunds-universitet/

[17] https://www.sverigesradio.se/artikel/iransk-man-utvisades-i-hemlighet-sags-som-hot-mot-rikets-sakerhet;https://www.sverigesradio.se/artikel/uppgifter-diplomat-pekades-ut-som-iransk-underrattelseofficer-av-sapo

2022, shed light on the regime's strategy of embedding operatives within educational institutions. The IRI actively infiltrates universities and think tanks illicitly to acquire research and technology, influence public opinion, and monitor dissident communities. Such operations align with the regime's wider geopolitical objectives, including evading international sanctions, surveilling opposition figures, and shaping policy in its favor.

The Illicit Acquisition of Research and Products

The IRI has repeatedly sought to obtain Swedish research, technology, and products through illicit means. By circumventing international sanctions, the regime has strengthened its economy and military while expanding its surveillance capabilities. Swedish authorities have uncovered multiple instances of illicit procurement directly linked to IRI officials.

- **1999**: A student in Sweden smuggled thyratrons—electronic components used in medical imaging andnuclear weapon detonation systems—to the IRI. To evade export controls, the student forged documents; authorities later uncovered the scheme.[18]

- **2002**: A diplomat at the IRI's embassy in Stockholm was expelled for attempting to obtain illicit materialswith potential applications in weapons production.[19] The incident illustrates the IRI's use of diplomatic cover to evade sanctions and conduct intelligence gathering.

- **2013:** A resident in the southern city of Lund attempted to export dual-use industrial valves to the IRI in violation of EU sanctions. These valves have applications in both oil refinement and uranium enrichment. Swedish authorities intercepted the shipment before it could be dispatched.[20]

---

[18] https://lucris.lub.lu.se/ws/portalfiles/portal/117350270/Ledningens_vilja_och_avsikt.pdf and https://www.dn.se/arkiv/inrikes/vapenutrustning-saldes-till-iran-21-arig-student-anhallen-pizzeria-utnyttjades-for-illegal-export/

[19] https://www.sverigesradio.se/artikel/137346

[20] https://www.svt.se/nyheter/lokalt/skane/salde-ventiler-till-iran-kan-ha-begatt-sanktionsbrott

These cases exemplify the Islamic Republic's broader geopolitical strategy: evading sanctions, obtaining cutting-edge technology, and exploiting diplomatic and academic channels to advance military and political objectives.

Hostage Diplomacy

Hostage-taking has become a routine instrument of statecraft for the IRI, including in its dealings with Sweden. Tehran arbitrarily detains foreign or dual nationals on politically motivated charges to extract concessions from other states.[21] In 2019, Swedish authorities arrested Hamid Noury, a former Iranian official, for his role in the 1988 mass executions of political prisoners. He was later convicted of war crimes and murder and sentenced to life imprisonment. In retaliation, the Islamic Republic escalated its use of hostage diplomacy by arresting Swedish citizen and European Union (EU) diplomat Johan Floderus in 2022 on fabricated espionage charges. The regime explicitly linked Floderus's imprisonment to Noury's. Its objective was to pressure Sweden into a prisoner exchange, which ultimately took place in June 2024.

The IRI's use of hostage diplomacy serves broader geopolitical aims: securing the release of its operatives in exchange for foreign detainees held unlawfully, extracting political and economic concessions, and intimidating Western governments to soften their positions on sanctions and human rights violations.

Cyber Attacks Against Individuals

The Iranian regime has routinely used data intrusion as a surveillance tactic against dissidents. As discussed in Part One (see the journal's previous issue), multiple IRI cyber operations have targeted regime opponents in Norway and Sweden. However, the regime's monitoring efforts extend beyond the Iranian diaspora to encompass non-Iranians whom the regime regards as strategically important for political and security reasons.

This section presents two case studies of data intrusion involving the authors of this paper. These examples provide a detailed account of how the IRI executed the attacks, illustrating its two-pronged approach to digital surveillance. The first strategy relies on large-scale intelligence-gathering operations targeting hundreds or even

[21] https://www.tv4.se/artikel/GRheIZVwtPhQ6LAhT2O42/irankaennaren-sa-utnyttjas-fangar-foer-att-saetta-press-pa-vaest

thousands of individuals. The second is more precise, focusing on select individuals through customized cyber operations. Together, these cases shed light on the regime's evolving cyber tactics and its sustained efforts to monitor and suppress its enemies.

The Case of Magnus Norell

In October 2022, Norell received an email from an individual claiming to be part of the Iranian legal team handling the Hamid Noury case. The sender identified himself as a professor of international law and requested permission to pose a few questions to Norell regarding the case. At that time, Noury had already been sentenced to life imprisonment for war crimes and murder.

A few days later, Norell got a WhatsApp call from a close friend in Iran who said he would soon receive emails from "the services" concerning Noury. In this context, "the services" referred to the Islamic Republic's security agencies—either the Intelligence Organization of the Islamic Revolutionary Guard Corps (IO-IRGC) or VAJA. Norell informed his friend that he had already been contacted about the matter.

Norell concluded that "the services" were pressuring his friend to act as an intermediary because his delayed response to the professor had aroused their suspicion. Their interest in him likely stemmed from his extensive work as a Middle East analyst, marked by frequent travel to the region and a broad network of contacts, making him a natural target for outreach.

Following these events, Norell reported the incident to Säpo by providing background information and updating the agency as new developments occurred. Over the ensuing months, he maintained irregular contact with the professor but eventually met him in spring 2023, when the professor was in Stockholm for meetings with Noury's Swedish legal team at the Thomas Bodström law firm.

In March 2023, Norell learned that a "Johan" was being held in Iran on espionage charges. This marked the first time he had heard of Johan Floderus and promptly reported the information to Säpo. Later that year, Floderus's imprisonment became public, apparently as part of the IRI's strategy to pressure the Swedish government into agreeing to a prisoner exchange. That exchange took place in June 2024, resulting in the release of Hamid Noury and positioning the

Islamic Republic as the primary beneficiary. Meanwhile, Swedish physician Ahmadreza Djalali remains imprisoned in Iran despite representing a more urgent case for a prisoner swap.

In early May 2024, a Säpo officer contacted Norell to request a meeting. During their discussion, the officer informed him that Norell had been the target of a cyber intrusion by "a foreign power." As part of the ongoing investigation, Säpo requested full access to his computer and subsequently uncovered evidence confirming the hack. When asked who he believed was behind the attack, Norell identified the Islamic Republic, a suspicion later corroborated by forensic analysis of his device.

Säpo also advised Norell to replace his router and computer immediately. However, during a follow-up meeting later in May, Norell surrendered his phone. He did so after experiencing additional intrusion attempts despite the earlier device replacements. These measures had at least temporarily disrupted IRI access.

Subsequently, in late May and early June, an attacker sent Norell an email falsely claiming to be from Stockholm University and inviting him to a conference. Norell, who called the professor listed as the sender, confirmed that the invitation was fake. Later in June, the attacker attempted the same tactic using a different email address and WhatsApp, again inviting him to a conference. In August, a third message was sent but this time via the email from one of Norell's closest friends. Each message contained attachments that Norell deliberately avoided opening, recognizing that such files often carry malware. In September 2024, authorities closed the investigation—a standard procedure when no prosecutable individual can be identified, mirroring Säpo's earlier response to the SMS attacks.

The Case of Arvin Khoshnood

During the summer of 2021, large-scale protests erupted in Khuzestan, Iran's oil-rich southwestern province. Initially triggered by severe water shortages and recurring power outages, the demonstrations rapidly escalated into a nationwide anti-regime movement, with protesters calling for the fall of the Islamic Republic. Unfolding amid the ongoing COVID-19 pandemic, these protests were part of a broader wave of anti-regime uprisings that had gained momentum since 2017–2018.

Throughout this period, Arvin Khoshnood actively disseminated information about the unfolding events in Iran. Drawing on a network of contacts within the country and the Iranian opposition, he shared timely updates via social media, briefed journalists and policymakers across Europe, and contributed to discussions on the protests' political and security implications. By this time, his extensive research and media engagement had established him as a frequent commentator on Iranian affairs.

On July 20, 2021, Khoshnood received an email from an emeritus professor at an Australian university proposing collaboration on two research projects related to human rights in Iran. The email included detailed descriptions of the projects, closely aligned with Khoshnood's expertise and prior publications. The message appeared legitimate, written in fluent academic English, and included a name, photograph, university affiliation, and contact number, all of which matched publicly available information. The only unusual detail was that the sender used a generic email provider rather than an institutional address; however, this was not inherently suspicious, as it is a relatively common practice among retired academics.

Later that day, Khoshnood replied, expressing interest in learning more about the proposed projects. On July 22, he received a follow-up email stating that university staff were preparing additional materials. Three days later, on July 25, the professor sent a PDF containing further details. The file appeared professionally formatted, resembling standard university templates, and included institutional logos, staff names, and a collaboration agreement with a link for more information. After reviewing the document and confirming that the listed staff members were indeed affiliated with the university, Khoshnood clicked on the link. Almost immediately, his computer displayed a warning message indicating an active cyberattack.

Reacting swiftly, Khoshnood shut down his computer and disconnected it from the internet before contacting IT security specialists. A technician who later examined the device described the incident as one of the most sophisticated phishing attempts he had encountered—a spear-phishing operation specifically engineered to extract login credentials. Given Khoshnood's prominent role in Iranian affairs, his extensive network of contacts within Iran and the opposition, and the highly targeted nature of the

attack, the technician concluded that the Islamic Republic was the likely perpetrator.

Seeking further clarification, Khoshnood contacted the Australian university and the real professor, who confirmed that at least two other Middle East researchers had been targeted in similar attacks. The professor had already reported these incidents to the university's security department, further supporting the likelihood that the phishing attack was part of a broader IRI intelligence operation. This was not the first time Khoshnood had been targeted. Over the years, he had received multiple threats aimed at discouraging his research on Iranian affairs. However, the July 2021 cyberattack stood out as one of the most direct and technically sophisticated attempts to compromise his work. Khoshnood believes the Islamic regime sought to access sensitive communications and uncover the identities of his sources. Despite these threats, he continues to observe strict security protocols to safeguard his contacts and data.

Conclusion

The IRI's intelligence operations in Scandinavia are extensive, systematic, and deeply embedded across Denmark, Norway, and Sweden. A comparative review of its activities in these countries reveals consistent patterns, particularly in the regime's reliance on espionage, cyber intrusions, extraterritorial repression, including assassinations, terrorism, and influence campaigns. Throughout Scandinavia, the regime's intelligence services actively monitor and intimidate dissidents, conduct cyberattacks on universities, and carry out covert influence operations through think tanks and academic institutions. These activities serve multiple purposes: gathering intelligence, silencing opposition voices, and circumventing sanctions to acquire sensitive technology. In addition, the IRI has planned terrorist activities on Scandinavian soil, most notably assassination plots against exiled dissidents and Jewish community members, as well as attacks on Israeli diplomatic missions.

The IRI's threats extend beyond the targeting of Iranian opposition figures and directly challenge the broader national security of Denmark, Norway, and Sweden. Its exploitation of criminal networks—such as Foxtrot—illustrates how the regime co-opts local actors to advance its objectives. Moreover, the regime's collaboration with Russia heightens concerns about

the wider geopolitical ramifications of its activities, particularly for European security.

Taken together, these developments indicate that the IRI's operations in Scandinavia are not isolated but components of a coordinated strategy aimed at exerting influence, suppressing dissent, and advancing its geopolitical agenda. Given the scale and severity of these threats, comprehensive and coordinated policy responses are essential to counter the regime's malign activities effectively.

Policy Recommendations

For decades, Scandinavian governments have responded passively to the IRI's intelligence operations. This perceived inaction has likely signaled weakness to the Islamic regime and other foreign actors monitoring the region. To strengthen Scandinavia's response and effectively deter future covert operations by Tehran, Scandinavian countries should coordinate closely and rapidly implement the following measures:

- **Consider closing Iranian diplomatic missions** unless the IRI ceases its covert activities. The regime consistently exploits its embassies as hubs for espionage, influence operations, and even terrorist activities.

- **Shut down IRI-linked mosques and Islamic centers** that function as fronts for intelligence gathering and ideological operations. These religious institutions are used to spread propaganda and conduct activities that threaten national security. In July 2024, German authorities set a precedent by closing the Islamic Center in Hamburg; Scandinavian governments should follow suit.

- **Advocate for the IRGC's designation as a terrorist organization** within the EU and European Economic Area. The IRGC plays a central role in the regime's intelligence, military, and terrorist operations. During the Joint Comprehensive Plan of Action (JCPOA), the Iranian Ministry of Foreign Affairs established a network to advance its influence, which included Rouzbeh Parsi, head of the Middle East program at the Swedish Institute of International Affairs. This network clearly indicates that IRGC influence extends far

beyond direct acts of violence.

- **Mandate thorough background checks at universities and research institutes** for staff and students from countries such as Iran or other states deemed hostile to Scandinavia. Denmark has already piloted vetting measures successfully at Aarhus University.

- **Impose stricter trade and financial sanctions** to curtail the IRI's operational capacity within Scandinavia and Europe. Tighten visa regulations for IRI officials to limit their regional access and influence.

- **Link these measures directly to demands** that the IRI immediately cease its military support for Russia's war against Ukraine.

Scandinavian governments should coordinate with other European countries where possible but must not allow their actions to be contingent on broader EU or international consensus. They must act decisively and in concert to counter IRI intelligence operations, defend national security, and prevent attacks on Iranian dissidents as well as other regime enemies and adversaries.

Arvin Khoshnood is a Sweden-based political scientist and researcher on Middle East security with a focus on Iran's domestic and foreign policy. Fluent in Farsi, he regularly provides analyses of Iranian politics to the media and advises policymakers, researchers, and journalists on regional affairs. He holds degrees in political science, human geography, and intelligence analysis from Lund University. He can be reached at arvin.khoshnood@gmail.com

Dr. Magnus Norell is a former adjunct scholar at the Washington Institute for Near East Policy in Washington, D.C.,a senior fellow at the European Foundation for Democracy in Brussels, and a research associate at the Wilfried Martens Centre for European Studies, also in Brussels. His research focuses primarily on international terrorism. Norell holds a Ph.D. in political science and peace and conflict research from Stockholm University. With abackground in military

and civil intelligence, he has worked extensively on counterterrorism and international terrorism. He can be reached at macmagnus@hotmail.com

Dr. Ardavan M. Khoshnood is an associate professor and senior lecturer of emergency medicine at Lund University in Sweden, as well as a criminologist specializing in offender profiling and violent crimes, including terrorism. His expertise also encompasses Iranian foreign policy, the Islamic Revolutionary Guard Corps (IRGC), and the Ministry of Intelligence. He holds degrees in political science from Malmö University, intelligence analysis from LundUniversity, and police work from Umeå University. He can be reached at ardavan.khoshnood@med.lu.se