Reichman University
International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

Not Only Nuclear - Iranian Espionage in Israel

Mr. Shalom Ben Hanan
August 2023

About the ICT

The International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world. Using a multidisciplinary arpproach, the ICT work to facilitate international cooperation in the global struggle against terrorism.

As an independent think-do-tank, the ICT focuses on themes realted terrorism, counter-terrorism, homeland security, threat vulnerability, risk assessment, intelligence analysis, national security, and defense policy.

Serving as a joint forum for international policymakers and scholars, the ICT draws upon the experiences of a comprehensive and international network of individuals and organizations with unique expertise on terrorism and counter-terrorism research, public policy analysis and education

In addition to publishing research papers, situation reports and academic publications for worldwide distribution, the ICT hosts a number of international seminars, workshops and conferences to discuss and educate followers on global and regional issues of security, defense, and public policy in order to better facilitate the exchange of perspectives, information and proposals for policy action.

Licensing & Distribution

Reichman University International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

ict.org.il
International Institute for Counter-Terrorism, (2023)

Not Only Nuclear - Iranian Espionage in Israel

Shalom Ben Hanan

On 11 August, 2023, Israeli media reported that the Shin Bet had successfully thwarted an Iranian espionage attempt on Israeli soil. An individual of Iranian descent, upon arriving at Ben Gurion Airport in Israel, was apprehended and subsequently interrogated by Shin Bet investigators. During the interrogation, the individual confessed to being recruited by Iranian intelligence and assigned to carry out espionage activities within Israel. Notably, the individual was instructed to acquire the specific intelligence targets only after entering Israel—a tactic commonly employed by Iranian intelligence to ensure the spy's successful infiltration into the country. Upon conducting a search of the spy's belongings, various espionage tools were discovered, including a concealed covert camera disguised as a tissue box, operational communication devices, and a sum of money.

The arrest and subsequent investigation present an opportunity to illuminate a crucial yet relatively obscure facet within the multifaceted rivalry between Israel and Iran. While the spotlight often centers on Iran's escalation of nuclear concerns, its backing of militant groups like Hezbollah and Hamas, its endeavors to establish a strategic foothold in Syria, and its readiness for a potential full-scale conflict with Israel, there exists another intricate realm referred to as state espionage.This realm encompasses not only traditional forms of espionage involving the recruitment and management of human agents (HUMINT), but also extends to incorporate cutting-edge techniques, including advanced technologies and an extensive utilization of the cyber domain. In the midst of the more prominently discussed elements, this undercurrent of state espionage constitutes a complex and significant component in the ongoing dynamics between the two nations.

One of the primary aims involves enlisting citizens for espionage objectives and procuring intelligence pertaining to diverse targets. The recruitment of an Iranian Jew and his dispatch to Israel serves as an illustrative instance of a multifaceted approach in action. Iranian intelligence employs tactics of influence to coerce Jewish residents within Iran into engaging in espionage ventures within Israel. This engagement might entail a direct solicitation of services or the enlistment of the individual to establish contact with relatives or associates based in Israel. Another stratagem entails reaching out to Israeli citizens via cyber channels and social networks, assuming the guise of an Iranian Jewish resident. Leveraging these digital platforms, the intelligence operatives establish connections and extend inquiries under various guises, such as business pursuits, academic research, journalism endeavors, or other fabricated narratives. These false identities become effective means to ensnare unsuspecting citizens,

who remain unaware that they're interacting with virtual agents of Iranian intelligence. Additionally, other target demographics comprise the Palestinian residents of the Territories and the Arab population in Israel. These groups might be approached either through the pretext of fabricated cover stories or directly, grounded in ideological motivations.

Contemporary advancements in technology do not replace the intrinsic human element, which remains a pivotal instrument for espionage and the gathering of intelligence. While the modern-day spy must make numerous adaptations to harness technology for the purpose of extracting high-quality information, the focus of espionage recruitment and operations remains centered on the capacity to influence individuals whose abilities, roles, or other skills contribute to the enhancement of intelligence gathering by the organization or country that recruited them. This scenario echoes the case of the spy who was arrested at Ben Gurion Airport at the beginning of the month of August 2023, whose recruitment hinged upon employing methods involving coercion and pressure exerted upon the Jewish community in Iran or their relatives residing in Israel. Furthermore, Iranian expatriates established within Israel, individuals in business circles, those with affiliations to security companies, soldiers within the military—particularly within intelligence units—and anyone identified by Iranian intelligence as possessing the aptitude for operational effectiveness and intelligence gathering, are also a target for the recruitment attempts of Iranian intelligence.

The internet, particularly social networks, serves as a pivotal platform through which Iranian intelligence conducts recruitment and espionage activities. The online realm offers unparalleled convenience, enabling anonymity, utilization of false identities, and the deployment of various cover stories, including those disguising business activities, all facilitated by secure and encrypted communications. In recent years, a number of attempts to activate individuals and networks have been exposed, revealing the Iranian intelligence's use of diverse cover narratives, primarily during the initial phases of activation. An illustrative case from 2022 involved the exposure of an Israeli citizen network operating within the Iranian intelligence apparatus. Notably, five members of this network were subsequently indicted. The investigation conducted by the Shin Bet uncovered that the network's interactions were orchestrated by a virtual operator who assumed a false identity, portraying himself as a Jewish resident of Iran. In more advanced stages of the operation, suspicions emerged among some network members regarding the involvement of Iranian intelligence. Despite these suspicions, they opted to sustain contact until eventual exposure and arrest. In other cases, inquiries initiated by virtual operators culminated in the point of contact within closed "WhatsApp" groups. These groups served as a conduit for sharing details about family members of interest to the Iranian operatives, with instructions occasionally being dispensed, even attempting to steer some family members toward enlisting in the Israeli Defense Forces (IDF) for roles within the Intelligence Division or for other seemingly innocuous tasks.

Another role that Iranian intelligence assumes within the cyber medium involves orchestrating a system of influence or manipulation, with the aim of inflaming the discourse of hate within Israeli society and exacerbating divisions across a spectrum of topics. This strategic endeavor requires substantial investment, as Iranian intelligence operates an array of websites, an army of automated bots, and thousands of fictitious profiles. Through these digital assets,

they actively intervene and shape discussions on social networks spanning a multitude of subjects. Furthermore, Iranian intelligence dedicates significant efforts and resources to the sphere of attacking and ompromising individuals' computers, cell phones, databases, and vital infrastructure within the borders of the State of Israel. In recent years, there has been a dramatic surge in the frequency of attacks targeting various critical systems, including hospitals, government databases, defense and civilian industries, financial institutions, insurance companies, research institutes, and more. Moreover, key political figures have had their mobile devices compromised in what appears to be a deliberate attempt to extract sensitive information.

These instances, among others, underscore a notable escalation in the extent of the Iranian threat within the realm of espionage, which constitutes a segment of the broader ongoing rivalry between Israel and Iran. The magnitude of this threat necessitates the diligent readiness of the Israeli security apparatus, the corporate domain, governmental entities, and even individual citizens. The foremost and fundamental facet of national preparedness revolves around enhancing awareness levels and imparting fundamental guidelines for recognizing and thwarting diverse threats through appropriate security measures and personal conduct. This includes adopting essential precautions and promptly notifying security authorities of any anomalies or suspicions.