2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

WHEN AVATARS COME ALIVE: UNDERSTANDING HYBRID THREAT ACTORS

Itay Cohen

Palo Alto Networks Unit 42, Israel

Omer Benjakob

Haaretz, Israel

itaycohen23@gmail.com
omerbj@gmail.com

ABSTRACT

Cyber influence as a unified threat has emerged as a key lesson from Israel and Iran's confrontations since 7 October 2023 and the war in Ukraine. Cyber espionage attacks converged with disinformation not just for online influence, but also for recruiting real-life agents, deploying them in the real world to sow chaos and, at times, even physically target officials based on data harvested online.

As a journalist and a threat intelligence researcher, we have experienced first hand how cyber and influence meshed and matured into real-world violence, receiving a death threat in the form of a package following the exposure of a wide-reaching cyber-enhanced disinformation campaign. Together we examine the offensive cyber-influence spectrum that has emerged during the war: from disinformation amplifying claims of widespread cyber attacks or hyping non-existent capabilities, to campaigns targeting Israelis' emotional reality and penetrating and disrupting their physical reality.

Our paper demonstrates how threat actors bridge the digital and physical domains, leveraging TTPs typically associated with APTs to orchestrate real-world actions. Combining investigative journalism, traditional threat intelligence methods, and exclusive access to unsealed indictments, we've correlated activities from online campaigns to tangible security threats, and uncovered the link between online personas and offline operatives.

We show how seemingly benign digital campaigns evolve into significant threats, as evidenced by Iranian operations that blurred the lines between espionage and trolling, directing local operatives to start fires and stir violence. Likewise, we examine how Russia's GRU integrates cyber-enabled disinformation and cyber attacks with on-the-ground sabotage and targeted violence, underscoring the wider landscape of hybrid threats. This investigative framework bridges digital and physical threats, offering actionable threat intelligence insights for tackling hybrid adversaries.

INTRODUCTION

In the world of Cold War espionage immortalized by John le Carré, human agents reign supreme – no satellite image can match the true value of a living, breathing human source, morally flawed or ideologically conflicted as they may be. But what happens when the cold digital dynamics of cyber warfare meet the chaotic unpredictability of human agents? The Iranian operations against Israel in the wake of October 7th 2023 and up until the end of the June 2025 war between the two countries offer a rich lesson on a new form of hybrid warfare that blurs the line between cyber and physical, between digital avatars and human agents, and between online trolls and real-world assassins.

We call them hybrid threat actors (HTAs), a term we conceptualize to denote state-sponsored groups, or proxy entities linked to states that conduct systemic operations across both digital and physical domains in a coordinated, convergent manner. The HTA can be understood as a subcategory or evolution of the advanced persistent threat (APT), expanding its operational scope beyond the purely digital realm. While conventional APTs focus on long-term cyber infiltration for espionage or disruption, HTAs blend these cyber operations with tactics from the world of influence and disinformation campaigns and kinetic actions into a unified and continuous kill-chain. They leverage cyber intrusions not just as end goals, but as preparatory stages – gathering intelligence, manipulating targets through social engineering – and thus facilitate real-world chaos, including sabotage and assassination.

This paper introduces and defines the concept of the hybrid threat actor (HTA). To provide a rich, in-depth exemplar for this model, we focus primarily on Iran's hybrid threat landscape vis-à-vis Israel from October 2023 until June 2025. To contextualize this as part of a broader evolution in modern warfare, the analysis also touches on other significant state-sponsored HTAs, mainly in Russia, whose GRU Unit 29155 has formally integrated a cyber warfare team to intertwine physical and digital tactics from inception.

BACKGROUND

Since mid-2023, Israel has witnessed an unprecedented wave of attacks aligned with what we and others have suggested can be seen as a new type of hybrid warfare, integrating cyber operations, online influence, and real-world deployment in a distinct new way.

Iran, this paper suggests, has found a way to translate TTPs usually associated with cyber or online warfare into physical actions. We note two distinct MOs: utilizing data collected from cyber intelligence into actionable intelligence, and utilizing communication channels initially used for disinformation and influence for enlisting and deploying agents – first digitally, then physically.

From 2023, Israel's policy toward such activities changed drastically: Israeli security bodies started to treat what were initially called 'cyber-influence' and foreign information manipulation and interference (FIMI) operations as an increasingly urgent national security threat [1]. No longer just an issue to be flagged by civil society organizations and lamented by online watchdogs concerned by disinformation on social media, Israel's secret Shin Bet security service began actively publishing cases of alleged agents being run remotely inside Israel by Iran on *Telegram* and on the streets.

As an investigative journalist focused on disinformation and cyber, and as a cybersecurity researcher focused on nation-state threat actors, both based in Israel, we have witnessed first hand how, when left unregulated, the online avatars behind disinformation campaigns metastasized into real-world threats: Israeli journalists and lawmakers have received

death threats [2], the families of Israelis being held hostage in Gaza received mock death notices [3] of their loves ones; Israeli cybersecurity researchers focused on Iran were doxxed, in tandem with a wave of hack-and-leaks [4] that exposed sensitive sites and the personal details of Israeli officials [5], potentially exposing them to harm. Iran, these incidents all highlighted, had managed to penetrate Israel, and Iranian cyber tactics – once contained to the digital realm – have evolved into sophisticated hybrid operations capable of real damage and chaos.

An OSINT analysis we conducted on official statements by Israeli bodies revealed that at least 23 Israelis were accused, suspected or arrested on charges that they were Iran-recruited operatives either preparing to execute missions on the ground or already doing so.

The Shin Bet recently confirmed that Iranian cyber campaigns have moved beyond surveillance into direct facilitation of assassination plots: in late 2024, the secretive security service revealed [6] that Iran had orchestrated some 200 targeted cyber attacks against Israeli security officials, politicians, academics and journalists. The goal was not mere data theft: attackers sought personal details (home addresses, routines, personal contacts) as part of plots to lead physical attacks on these targets. Shin Bet officials warned [7] that the stolen information was intended to 'serve the Iranians in carrying out an assassination of individuals in Israel, via local cells recruited in-country'.

This case exemplifies how a digital intrusion (hacking for intel) can feed directly into a kinetic plot (deploying hit teams), blurring the line between cyber espionage and traditional terror tactics. This pattern of cyber-based kinetic attacks was further seen in the foiled plot to assassinate former Defence Minister and IDF Chief of Staff Moshe Ya'alon. In September 2023, a plan to kill [8] Ya'alon during his morning run in Tel Aviv's Yarkon Park was made public. An investigation revealed that a local Hezbollah cell, acting as a proxy for Iran, had gathered intelligence on his daily routine. Locally run operatives planted an Iranian-made Claymore mine (smuggled into the country) along his presumed path and even attached a camera to the IED, allowing them to remotely monitor the park trails and detonate the bomb when they spotted him. The plot – foiled when the device exploded prematurely without causing any injury – demonstrates a clear operational model: using intelligence to enable a violent, kinetic attack by a proxy force.

Similar dynamics are now playing out by Iran in other arenas. Iranian state actors have used cyber espionage to directly facilitate assassination and revenge operations in the US: since 2021, IRGC-linked hackers (often tracked as APT42/Charming Kitten) have repeatedly tried to breach [9] the personal email accounts and devices of former US officials from the Trump administration. US intelligence assesses this campaign as part of Tehran's effort to locate and retaliate against those officials for the 2020 killing of IRGC General Qasem Soleimani [10]. John Bolton – Trump's former National Security Advisor and a known Iran hawk – confirmed that Iranian hackers sought access to his data and schedules, noting that 'access to somebody's schedule could be very, very helpful to the Iranians' in planning an attack. Indeed, in one plot foiled in 2024, a man with ties to Iran tried to hire hitmen to assassinate a US politician, a scheme US authorities described as 'straight out of the Iranian playbook'. This demonstrates a concrete linkage: cyber intrusions to steal personal info and tracking data directly enabled IRGC assassination teams to identify, locate, and attempt to kill their targets on Western soil.

THE DISINFORMATION-TO-RECRUITMENT PIPELINE

Reviewing statements made by Israel's Shin Bet, as well as indictments filed against Israelis who were enlisted as part of what we call the Iranian hybrid-threat-pipeline, and cross-referencing them with media reports and OSINT materials, shows how Iran has weaponized platforms like *Telegram*. This weaponization goes beyond known threats such as psychological or influence warfare, and turns them into direct recruitment platforms for agents tasked with HTA operations.

The digital platforms favoured by Iran for HTA operations serve not only for spreading disinformation or amplifying hack-and-leak drops, but also for active recruitment of agents – witting or unwitting. In fact, these work hand in hand: *Telegram*, possibly due its perceived anonymity, as well as its popularity among Russian-speaking users, has emerged as a key node in the local disinformation-HTA pipeline.

These recruited agents, if they can be called that, are typically vulnerable Israelis, marginalized communities, and immigrants more susceptible to economic and other forms of persuasion – yet we argue their operational logic is more that of digital botnets than spies. The underlying recruitment strategy is disturbingly simple, yet effective: exploit social isolation, financial desperation, and criminal histories to push recruits toward escalating violence, fuelled and supported by a rich and well documented list of offensive cyber activities.

Over the past 18 months the Shin Bet has revealed a number of cases showing how Israelis were being recruited on *Telegram* by the same accounts social media researchers [11] had previously linked to cyber influence campaigns intended to exacerbate existing social tensions online. In one case, the user names used by the Iranian avatars and the names of the channels they operated were doxxed by Israel as part of a growing campaign to warn the public against the new threat.

For reporters covering disinformation they confirmed what had long been anecdotally reported: Iran was using *Telegram* in new and creative ways, going beyond simple 'influence' and 'disinformation'. Reports [12] by *Haaretz* showed how disinformation-focused avatars, likely run by Iranian agents, not just ran their own groups but also tried to penetrate groups of activists and, once inside, tried to get them to conduct different actions on their behalf. The Shin Bet, once reluctant to comment on such domestic issues, began to voice [13] concern at 'Iranian' networks operating on Israeli messaging platforms.

Online recruitment often begins with low-stakes provocations – posting inflammatory slogans or graffiti for small payments – but rapidly advances to acts of sabotage, arson, espionage, and even assassination plots. Fake employment offers on *Telegram* and social media were common starting points [14], quickly pivoting into demands for increasingly aggressive physical actions [15]. Some were tasked with passing on cash to more serious agents, others with trying to recruit others into the pipeline.

CASE STUDIES: HTAS IN ISRAEL (2023 - 2024)

The material escalation of Iranian influence operations from digital interactions into real-world violence is strikingly clear when reviewing the procession of incidents made public by the Shin Bet, going from general statements to doxxing specific groups and accounts on *Telegram* that had both pushed out disinformation and set up fake online assets for recruiting Israelis. These also included not only job posting channels, but also purported swinger parties. Reviewing the posts made public [14] by the Shin Bet, as well as others found by FakeReporer, an Israeli disinformation watchdog, shows that while initial digital contact can appear innocuous, offering attractive but vague 'job opportunities', the reality rapidly becomes darker.

Figure 1: One of the advertisements revealed by Google to have been targeting Israelis for fake jobs posted by Iranian intelligence. Credit: Mandiant/Google Cloud.

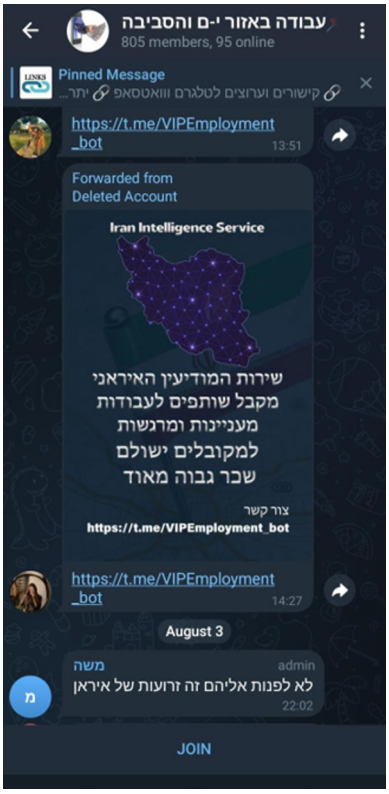

Figure 2: One of the Telegram channels revealed by the Shin Bet to have been Iranian intelligence recruiting Israelis. Credit: Shin Bet via Haaretz.

Initially, these seemed limited to the digital arena, with agents asked to help troll Israeli messaging apps: for example, images taken by witting and unwitting agents were posted on social media channels seemingly geared solely at psy-ops, an example of how Iran can 'get anywhere' inside Israel. However, over the following months, the Shin Bet would reveal a number of cases showing how Israelis were being recruited on *Telegram* by the same accounts social media researchers [11] linked to seemingly benign cyber influence campaigns, and these individuals were being sent out to 'troll' [16] not just social media but Israel, using graffiti to amplify their online content IRL.

A positive feedback loop between physical and digital influence efforts seems to emerge. For example, Elimelech Stern [17] (see Appendix case 3), a young Hasidic Jew from the religious Israeli town of Beit Shemesh, was recruited by an Iranian operative masquerading as a woman named 'Anna'. 'Anna' was part of a group of avatars that were using Israeli burner numbers to try to penetrate different groups on *Telegram* as well as hosting their own channels and groups. They directed the Hasid not only to print inflammatory posters, in line with the messages being pushed out on social media, but also to undertake symbolic, yet provocative acts in reality. These, too, would soon grow violent and would include threatening Israeli officials – at times in alarming, yet somewhat comical ways. Stern's online handler suggested delivering a sheep's head as a physical threat. Such incidents have repeated themselves over the past 15 months, showing how trolling, online or offline, contains a violent seed that if left untended can rapidly escalate.

Another such case is that of Eden Dabas [18] from Ramat Gan (see Appendix case 4), which epitomized the escalating threat: on 5 August 2024, the Shin Bet and police arrested Dabas for carrying out missions at the behest of an Iranian agent. Dabas had been approached online and instructed to buy a dedicated phone and SIM card for covert communications. He was then tasked with printing and posting (which he proceeded to do) inciting flyers in Israeli cities – including posters calling for a military coup. This is exactly in line with the narratives being pushed out by the Iranian influence groups (such as Second Israel and Tears of War) exposed by the Shin Bet and social media researchers. These groups and the avatars running them also used specially purchased Israeli burner numbers and were later linked to more violent forms of trolling, including death threats sent to reporters and Israelis.

Dabas, much like the avatars, was then tasked with setting up a *Telegram* channel aimed at recruiting additional Israelis to spy for Iran, underscoring the memetic and viral nature of HTAs. Dabas purportedly created over 2,000 fake social media profiles to amplify Iranian narratives. According to his indictment, he was tasked with more serious and kinetic provocations: his handler directed him, for instance, to torch cars and even to place a severed animal head near the home of an Israeli official. Dabas received approximately $12,000 in payments from his Iranian handler for these missions, most of which Dabas only pretended to carry out. He reported these tasks as done to his operators, without actually doing them – a case of disinformation on disinformation that also helps underscore how low in actual value such 'agents' are, even in the most willing of cases. They also show Iran's digital recruitment MO – pushing operatives to their limits, testing the boundaries of their willingness, and assessing their operational reliability on an ever escalating spectrum of tasks that seem to follow a logic more closely linked to the world of cyber rather than classic warfare or intelligence.

From vandalism to violent plots

The case of Vladislav (Viktorson) Viktorov [19] (see Appendix case 6) and Anna Bernstein (see Appendix case 7) dramatically illustrates [20] this dangerous trajectory. A convicted rapist in his 30s and his younger partner were recruited via *Telegram* groups Viktorov frequented. Initially tasked with minor vandalism – such as spray-painting anti-government slogans for small payments – their Iranian handlers swiftly escalated demands, offering bigger sums for bigger asks. They were tasked with setting random vehicles ablaze in Tel Aviv and vandalizing banks. Viktorov was also given the somewhat comical task of trying to find homeless people willing to start random fires themselves, offering each $20 a pop. This was both a test of his loyalty and an attempt to cause random panic in Israel – a form of physical and dangerous trolling. Each successfully completed task increased the pair's perceived reliability in the eyes of their handlers, eventually culminating in suggestions Viktorov commit an assassination – a mission the convicted sex offender was unwilling to carry out.

The transition from digital provocations to physical violence and real-world surveillance has marked Iranian operations in Israel with alarming consistency. While initial activities resembled the typical antics of internet trolls and hackers (like spray-painting incendiary slogans and website defacements) this low-level vandalism quickly escalated into far more severe threats, underscoring how digital influence tactics can mature into tangible national security threats.

Similarly troubling was the case of Vladimir Varkhovsky [21] (see Appendix case 8), who resided in Tel Aviv. Varkhovsky was approached via *Telegram* by Iranian operatives masquerading as Israeli expats. He began with low-stakes assignments: graffiti targeting Netanyahu and surveillance of anti-government protests. The escalation was textbook – soon Varkhovsky was directed to procure an unregistered handgun. Offered $100,000 and a safe exfiltration to Russia, his assignment was specific: the assassination of an Israeli scientist. Thankfully, his preparatory actions – visiting the target's neighbourhood, mapping routines, and finally picking up a covertly delivered pistol – were intercepted by Israeli authorities. The immediacy and directness of these threats illustrated how swiftly digital prompts could manifest into real-world dangers.

FROM INTELLIGENCE GATHERING TO ACTION

Parallel to its recruitment of ground-level proxies, Iran conducts sophisticated cyber espionage campaigns with a clear and stated purpose: to gather the necessary intelligence for planning and executing physical attacks. These operations are not for abstract strategic advantage but are a direct preparatory phase for real-world targeting, transforming stolen data into actionable intelligence for assassinations, kidnappings and surveillance.

This strategic linkage has been explicitly confirmed by Israeli security services: the Shin Bet has repeatedly stated that the goal of Iranian phishing and hacking campaigns is to collect sensitive personal information – including home addresses, daily routines and social connections – to enable physical attacks against targeted individuals inside Israel, often utilizing the very same types of locally recruited cells as described previously. This official assessment provides a direct, authoritative bridge between the cyber and kinetic domains. The TTPs employed in these espionage campaigns are tailored for maximum effectiveness against high-value human targets. A primary method is spear-phishing, often involving intricate social engineering and impersonation. Iran-linked threat groups, such as the one tracked as Phosphorus, have demonstrated the capability to conduct highly targeted campaigns.

In a parallel campaign [22], Iranian hackers breached the personal email accounts of multiple Israeli officials – including a retired major-general, a former US ambassador, and ex-foreign minister Tzipi Livni – then impersonated them to siphon sensitive data from other high-rank contacts. Stolen correspondence, passport scans, and conference registration details allowed the attackers to craft laser-accurate invitations – complete with flight preferences and hotel choices – dramatically raising the odds that a victim would accept. Israeli security officials say these two streams are tightly linked: the phishing-and-impersonation wave provided the intelligence that made the social-engineering covers so convincing, while the fabricated conference invites offered a pretext to harvest yet more credentials and travel data. Dozens of abduction plots were ultimately foiled, but the scheme illustrates a seamless chain from digital breach to physical threat – the inbox becomes the on-ramp to an ambush, exemplifying how Iranian cyber operations and real-world violence now operate in lockstep.

In one notable case, attackers compromised the authentic email account of a well-known former IDF general. They then hijacked an existing email conversation with Livni to send a malicious link, leveraging the established trust between the two parties to bypass suspicion. In another instance, Iranian operatives hacked the computer of veteran journalist Ehud Yaari by posing as former US envoy Jason Greenblatt and sending a policy paper on Gaza as a lure. The impersonation of high-level officials is a recurring theme, with operatives also posing this year as Israeli Cabinet Secretary Yossi Fuchs [23] in an attempt to solicit information from another Israeli citizen.

The data sought in these attacks is specifically that which is most useful for physical operational planning. Attackers aim to exfiltrate:

- **Credentials**: Gaining access to primary email accounts serves as a pivot point to compromise other services, uncovering a trove of sensitive personal and professional data.
- **Identity documents**: Campaigns have been designed to trick victims into uploading scans of their passports, using legitimate-looking identity verification services as a front. These documents are invaluable for identity theft, creating fraudulent travel documents, or other logistical aspects of a physical operation.
- **Location data and routines**: By compromising a target's primary *Google* or other cloud account, attackers gain access to a wealth of pattern-of-life intelligence, including location history, calendar appointments, and contact lists, all of which are critical for planning surveillance or an assassination.

A particularly insidious tactic involves luring targets abroad with invitations to fictitious overseas conferences or events. In one such scheme, Iranian agents created an elaborate persona of a European think-tank organizer who contacted former Israeli security officers with an offer to speak at a (fictitious) conference in Europe. Other ploys included impersonating a well-known Russian-Jewish billionaire philanthropist to offer partnerships, and a British journalist seeking interviews. These approaches were all socially engineered via email, *LinkedIn* and *Telegram*. If the targets took the bait, they would be flown abroad where Iranian handlers lay in wait. The Shin Bet ultimately thwarted dozens of these attempts, noting that the operatives' cover stories were tailored to each victim's background – a precision that would not be possible without extensive cyber reconnaissance.

These espionage operations must be re-contextualized beyond traditional intelligence gathering. They represent the active development of a 'kinetic targeting package'. The process of a methodical collection of tactical data required to execute a physical mission. The intelligence gathered in the digital realm directly enables the actions of operatives in the physical world. We see how the real-world agents are given similar tasks by the avatar operators: Varkhovsky was tasked with preparatory actions such as visiting his assassination target's neighbourhood and mapping their routines. These are precisely the actions that would be facilitated by the successful exfiltration of data from the target's personal accounts. Therefore, the cyber espionage campaign is not a separate activity; in much the same way the agent's actions are not just physical, they are part of a cyber kinetic kill chain.

Hack-and-leak and tactical doxxing

Hack-and-leak tactics have traditionally served as a strategic endpoint: hackers quietly infiltrate targets, exfiltrate sensitive

data, and then strategically release it publicly to cause reputational harm, political instability, or to manipulate public discourse. However, within the HTA framework described herein, hack-and-leak becomes more than an endpoint – it transforms into a tactical phase that not only amplifies online psychological influence but also signals kinetic operations on the ground.

Groups such as the Iranian-linked 'Handala' illustrate how hack-and-leak campaigns can serve multiple operational functions simultaneously. In mid-2023, Handala, widely identified by researchers and Israeli security services as affiliated with Iranian cyber actors, orchestrated a series of leaks targeting Israeli entities. According to reporting by *Haaretz* and others, Handala specifically targeted sensitive personal data of Israeli security officials, military personnel, and journalists. These leaks didn't merely aim at humiliation or reputational damage. Instead, they explicitly published home addresses, private phone numbers, email addresses, and family details, aligning closely with the known Iranian operational objective of kinetic targeting and de facto doxxing targets for their agents and others to target, directly supporting Iran's broader strategy of kinetic targeting – physical intimidation or attacks against specific individuals.

In February 2025, Iranian-linked hackers took what was perhaps the most brazen step yet in signal-based hack-and-leak campaigns when they breached a central Israeli database of civilian gun licences – leaking the full names, addresses, firearm types, ammunition counts, and even storage locations of over 10,000 licensed gun owners [24]. The leak was promptly echoed across Iranian-affiliated accounts and on leak platforms akin to *WikiLeaks*. The exposed registry transformed a benign database into a 'targeting registry', enabling hostile actors – whether criminal or state-sponsored – to profile and locate armed civilians, potentially intercepting or neutralizing them physically. This leak follows the HTA pattern exactly: cyber intrusion yields a public action, in this case a data dump that energizes potential kinetic operatives with a list of targets and their locations. Israeli authorities have reported that some of the Iranian recruited agents were tasked with collecting guns and ammunition from pick-up spots.

However, the seriousness of these threats doesn't mean all hack-and-leak incidents should be taken at face value. Recent cyber activities following geopolitical tensions, such as the October 7th attacks in Israel, reveal a troubling pattern of exaggerated claims by hacktivist groups, many hosting Iranian leaks. Many attackers focus more on generating media attention than achieving genuine technical breakthroughs. For instance, low-effort 'soft attacks' such as compromising a single email inbox or executing basic phishing campaigns are often exaggerated as significant breaches through flashy propaganda and aggressive media campaigns like those pushed out by Handala over the past year.

Airbase surveillance: from phishing to hacked cameras and on-ground spies

One particularly telling case unfolded around the Israeli Air Force's Nevatim Airbase at the start of the war. In October 2023, Iranian-affiliated cyber persona 'Soldiers of Solomon' [25] claimed responsibility for breaching and leaking surveillance camera footage, purportedly from inside Nevatim, considered a sensitive site. The leak was part of Iran's cyber-psychological warfare campaign. Analysts later determined that the footage actually originated from a civilian area named Nevatim Street, north of Tel Aviv, not from the base itself – though the claim still served to sow fear and confusion.

Less than a year later, in September 2024, a major espionage operation emerged from Haifa, where Israeli authorities arrested [26] seven Israeli citizens – immigrants from Azerbaijan – who were all allegedly part of a major espionage operation under Iranian guidance. The Shin Bet, Israel's internal security service, charged the group with conducting surveillance on critical sites across Israel. Their handlers, known only as 'Alkhan' and 'Orkhan', meticulously directed them to surveil military installations like Nevatim Airbase, along with Ramat David, Tel Nof and Palmachim airbases, multiple Iron Dome batteries, and civilian infrastructure including major seaports and power plants. They carefully documented damage sites following rocket attacks to refine Iranian targeting. Beyond infrastructure, they also surveilled prominent individuals, gathering extensive personal data to facilitate potential kidnappings or assassinations. Over a two-year span (2022 - 2024), they carried out approximately 600 missions, retrieving photos and details for their Iranian handlers, reportedly assisting missile-strike planning.

Notably, footage and satellite analysis later confirmed Nevatim was struck during Iran's 1 October 2024 ballistic missile attack – part of 'Operation True Promise II' – causing minor, but widely reported damage. The convergence is striking: a two-pronged strategy, combining cyber intrusion and human espionage, targeting the same military assets. The leaked CCTV fostered psychological pressure, while the ground-level surveillance apparently informed human operations that were also pushed out on social media.

THE BIRTH OF CADET BLIZZARD: A LANDMARK FUSION OF CAPABILITIES

Russia's GRU Unit 29155 [27] has an infamous pedigree for violent covert action – its operatives have been linked to the poisoning of Sergei Skripal in 2018, a fatal bombing of an arms depot in the Czech Republic, a coup attempt in Montenegro, and other acts of sabotage and assassination across Europe. In a significant evolution of this model, the unit has now fully integrated an in-house cyber warfare team, deliberately intertwining physical and digital tactics. This fusion was officially exposed in a landmark September 2024 joint advisory [28] by CISA, the FBI, NSA and a coalition of Western intelligence agencies, which identified the APT group Cadet Blizzard (a.k.a. Ruinous Ursa/Bleeding Bear/UNC2589) as 'an organic part of Unit 29155'. This formal attribution confirmed that, since at least 2020, these GRU

hackers have augmented traditional special forces missions with cyber operations aimed at espionage, sabotage and influence. In the stark words of the joint advisory, 'FBI, NSA, and CISA assess Unit 29155 is responsible for attempted coups, sabotage and influence operations, and assassination attempts throughout Europe. Unit 29155 expanded their tradecraft to include offensive cyber operations since at least 2020.'

This formalization of a cyber wing within a premier kinetic unit represents a critical development. The GRU maintains [29] other, more established cyber units, such as Unit 26165 (Fancy Bear) and Unit 74455 (Sandworm), which are primarily cyber-focused organizations. The decision to embed a new cyber capability directly within Unit 29155, rather than having it cooperate with existing cyber units, points to a deeper strategic logic. This organizational structure implies that hybrid operations are not an afterthought or a support function for Unit 29155. Instead, mission planning is likely inherently hybrid from its inception. An operational plan conceived within this unit would logically integrate cyber effects (e.g. disrupting communications, wiping data, conducting surveillance) and physical effects (e.g. planting an explosive, carrying out an assassination) as co-equal elements of a single mission, executed by a single, unified command structure. This represents a mature, formalized military doctrine for hybrid warfare, designed for seamless integration with conventional military campaigns and other instruments of national power.

The devastating effectiveness of this integrated doctrine was put on full display with the opening salvos of Russia's full-scale invasion of Ukraine. Unit 29155's cyber wing, Cadet Blizzard, launched some of the first attacks of the war, deploying the destructive WhisperGate wiper malware against dozens of Ukrainian government and critical infrastructure targets on or around 13 January 2022 – just weeks before Russia's physical assault on 24 February.

This was a textbook HTA operation, synchronizing cyber and kinetic effects. The WhisperGate malware was not ransomware, despite its initial appearance; it was a purely destructive cyber weapon designed to render systems inoperable. It functioned by overwriting the master boot record (MBR) of infected machines, making them unbootable, and then corrupting files with certain extensions, permanently destroying the underlying data. The cyber attack was accompanied by website defacements that displayed provocative messages in Ukrainian, Polish, and Russian, including the phrase 'be afraid and expect the worst', and falsely claimed that citizens' personal data had been leaked online.

This was a clear act of battlefield preparation. By destroying data, disrupting networks, and spreading fear and confusion, the WhisperGate attack helped to degrade Ukrainian command and control, impair communications between government agencies, and sow chaos among the civilian population at the precise moment that Russian conventional forces were massing at the border. The cyber operation was not a standalone event; it was a preparatory action, carefully timed and executed to shape the physical battlespace and create advantageous conditions for the subsequent military invasion. This demonstrates the core principle of the Russian HTA model: the use of integrated cyber-kinetic operations as a potent force multiplier in state-on-state conflict.

USING HACKTIVISM FOR AMPLIFICATION

The phenomenon of 'fake hacktivism', where nation-state actors masquerade as independent cyber activists, adds another layer of complexity. Russia, Iran and North Korea have all been accused of using this tactic to obfuscate their involvement in certain operations. By cloaking themselves in the guise of grassroots activism, these nation-states can pursue their political agendas under a veneer of plausible deniability. These groups use hack-and-leak tactics as precursors to physical sabotage, embedding digital espionage within a broader operational context. The leaks facilitate timing and coordination of kinetic actions, demonstrating an advanced operational logic that directly contrasts with the over-hyped yet technically superficial actions typical of other hacktivist activities. However, within the HTA framework, this tactic serves a purpose far beyond simple misdirection, it is a core component of psychological warfare and operational amplification.

Iranian HTAs in particular harness this model effectively. They exploit digital platforms, notably *Telegram*, and an array of cyber capabilities in a way that effectively bridges the gap between digital and physical, between digital influence operations and tangible threats. Following geopolitical events like the October 7th attacks, there is often a surge in cyber activities that are hyped to appear more significant than they are. This reveals a troubling trend: attackers inflating their impact through media manipulation rather than meaningful technical prowess. At first glance, some of these 'hacktivist' operations present grave security threats, with claims of widespread data breaches or the disruption of critical infrastructure. Yet, on closer inspection, many are the result of relatively unsophisticated intrusions – the cyber equivalent of 'more show than go'.

These attackers have become adept at packaging low-effort intrusions, such as compromising a single email inbox or deploying basic malware, as larger-than-life operations. They often focus more on producing flashy propaganda videos and aggressive media campaigns than on conducting technically meaningful cyber operations. The goal is not always to cripple networks but to create the illusion of omnipresence and foster a perception of chaos and insecurity where it may not truly exist. The success of these campaigns is measured not by their immediate technical effects, but by the media coverage and public panic they generate.

This raises a critical question for analysts: should we take these groups at their word? The answer is never without proof. Ransomware groups are notorious for inflating their successes, and the same holds true for state-sponsored actors posing as hacktivists. Their ultimate goal is often media attention, not material impact.

For Iranian HTAs, the use of 'fake hacktivism' is a calculated strategy. The noise and media hysteria generated by these over-hyped, low-sophistication attacks create a smokescreen that can distract from more serious, methodical operations such as the threats laid out here. Furthermore, the constant barrage of seemingly successful attacks, even if minor, contributes to a broader atmosphere of fear and vulnerability, which is a primary objective of influence operations that are aided by the physical operations conducted by HTAs.

Therefore, while acknowledging the tendency to inflate cyber threats, it remains critical to differentiate between different types of attacks: first between performative attacks designed for amplification and genuine hack-and-leak operations that serve as precursors to kinetic action, and between online influence and physical recruitment and deployment efforts. The leaks that expose personal data of officials or the locations of armed citizens are not mere propaganda; they are tactical intelligence dumps that facilitate physical threats. Thus, while acknowledging the tendency to inflate cyber threats for media attention, it remains critical to recognize when leaks transcend propaganda in the same way as it is critical to recognize when avatars can grow violent.

CONCLUSION

For too long, we have accepted a superficial and increasingly false dichotomy between the physical and the digital, between cyber and terror, between influence operations and kinetic threats. This divide has informed policy and delineated cybersecurity research from disinformation research and from other security-focused disciplines. It also created a lacuna that has left hybrid threats misdiagnosed and allowed the conditions that foster them to fester. In Israel, the aftermath of the October 7th attacks exposed the cost of this blind spot: the Iranian HTA model shattered conventional distinctions and what was once considered 'just influence' or 'only disinformation' has proven itself an operational precursor to violence. The failure to bridge the gap between cybersecurity, disinformation, and counterterrorism created fertile ground for a new kind of warfare – one Israel was ill-prepared to face.

The dominant discourse around avatars and bots remains mired in the language of platform governance: FIMI, DIMI, content moderation, trust and safety. But avatars – especially those deployed by Iranian-linked HTAs – are not just online actors: they recruit, radicalize, and reroute digital behaviour into physical missions. Treating avatars as 'content moderation' problems rather than national security threats is a mistake. These are not fringe anomalies but structured instruments that continued Iranian cyber warfare in the physical world. We need frameworks that recognize that avatars are part of a wider threat chain.

The vulnerability they exploit is one that is prevalent across the West; victims of this manipulative recruitment often fit a clear profile. They're isolated individuals, financially or socially vulnerable, frequently with criminal records or troubled pasts, in many cases immigrants or those desperate for a new identity and already spending ample time on alternative news channels on platforms like *Telegram*. Vladislav Viktorov (formerly Koklin) exemplifies this pattern vividly. A convicted sex offender, Viktorov was notably desperate to erase his past, adopting a new identity and eagerly embracing Iran's online outreach. Like an avatar recreating his real identity, he was born anew. His tasks began simply: spray-painting anti-government slogans for $20 apiece, the same price he would then be told to offer for arsons. The escalation – setting cars ablaze, vandalizing ATMs, even entertaining assassination attempts – speaks volumes about the vulnerability Iran exploits in its digital recruits.

This approach mirrors precisely how online troll farms and bot networks function. Personas initially created to disseminate propaganda or misinformation transition seamlessly into instruments of real-world chaos. Like digital bots switching identities to adapt to new campaigns, Viktorov adopted new personas to evade detection. The cycle of digital influence and real-world sabotage underscores a critical vulnerability: treating these operations as isolated incidents or low-level vandalism severely underestimates their strategic potential.

Thus, the analytical HTA framework that suggests viewing these actors as 'bots come alive' is particularly useful for threat intelligence practitioners. It reframes our understanding of hybrid threats, forcing recognition of influence operations not as peripheral annoyances, but as central components in a broader operational chain leading directly to national security threats. Iran's meticulous exploitation of digital infrastructure to recruit, radicalize, and deploy agents demonstrates a sophisticated strategy designed to maximize psychological and physical impact – confirming that today's 'bots' can indeed transform into tomorrow's spies and saboteurs.

Understanding these HTA operations requires reframing our perception of digital influence and reforming the disinformation discourse, currently still limited to debates about social media and severely restricted due to their interests. Treating these campaigns as mere online annoyances misses their dangerous evolution into serious national security threats.

To counter these threats, we must bridge the methodological divides between cybersecurity and intelligence, disinformation and national security, trolls and potential terrorists.

APPENDIX

List of suspected espionage incidents in Israel (October 2023 to June 2025):

1. Dmitry Cohen, 27 May 2024, Shin Bet – Photographed IDF sites, paid in crypto [30].
2. Tel Aviv man (unnamed), June 2024, Shin Bet – *Telegram* recruitment, documented targets, graffiti [30].

3. Elimelech Stern, 9 July 2024, Shin Bet + Lahav 433 – Posters, threat to diplomat [17].
4. Eden Dabas, 5 August 2024, Shin Bet + Tel Aviv District Police – *Telegram* channel, incitement, online influence, payment and more [18].
5. Mordechai (Moti) Maman, 28 September 2024, Shin Bet + Lahav 433 – Travelled to Iran, planned attacks [31].
6. Vladislav Viktorov, 4 October 2024, Shin Bet – Graffiti, arson, attempted terror [19].
7. Anna Bernstein, 4 October 2024, Shin Bet – Accomplice in arson, threats [20].
8. Vladimir Varkhovsky, 11 October 2024, Shin Bet + National Fraud Unit – Graffiti, tried to obtain gun [21].
9. Seven unnamed Azerbaijani-Israelis (Haifa area), October 2024, Shin Bet – Recruited via *Telegram*, spy ring that surveilled military installations, and passed info to Iran for three years [26].
10. Seven unnamed East Jerusalem residents, October 2024, Shin Bet – Pro-Iran graffiti, planned assassinations [32].
11. Rafael & Lala Guliev, October 2024, Shin Bet – Monitored researcher, took photos, espionage for Iran [33].
12. Asher Benjamin Weiss, October 2024, Shin Bet – Monitored Israeli nuclear scientist, sabotage intent [21].
13. Artyom Zolotrev, November 2024, Shin Bet – Graffiti, arson, target list [32].
14. Israel (Ardalar) Amoyal, November 2024, Shin Bet – Pro-Iran graffiti, attempted terror [32].
15. Yuri Eliaspov & Georgi Andreev, January 2025, Shin Bet – Leaked Iron Dome info from IDF [30].
16. Doron Buchovza, March 2025, Shin Bet + Lahav 433 – Sent nuclear info to Iranian contact, was fake [34].
17. Roi Mizrahi & Almog Attias, May 2025, Shin Bet – Planted bomb, planned attack on defence minister [35].
18. Unnamed 13-year-old boy, June 2025, Shin Bet – Recruited via *Telegram*, asked to document Iron Dome [36].
19. Unnamed Tel Aviv man, June 2025, Shin Bet – Took photos of IDF bases for money [35].
20. Alleged spy for Iran placed powerful explosives near defence minister's home [37].
21. Caught on camera: The young men from Nesher suspected of spying for Iran in action [38].

REFERENCES

[1] Breiner, J. Analysis | How Israelis Are Lured Into Spying for Iran. Haaretz. 22 October 2024. https://www.haaretz.com/middle-east-news/iran/2024-10-22/ty-article/.premium/how-israelis-are-lured-into-spying-for-iran/00000192-b48e-d542-a9ba-b5cf68520000.

[2] Benjakob, O.; Peleg, B. Fake Photos and Persian Accents: Foreign Psyop Groups Send Death Threats to Israeli Journalists. Haaretz. 4 June 2024. https://www.haaretz.com/israel-news/2024-06-04/ty-article/.premium/fake-photos-persian-accents-foreign-psyop-groups-send-death-threats-to-israeli-reporters/0000018f-dfb8-db29-a3ef-ffba45ef0000.

[3] i24 NEWS. Family of hostage receives mysterious funeral wreath – initial Shin Bet investigation suggests Iranian agents. 7 April 2024. https://www.i24news.tv/en/news/israel-at-war/artc-family-of-hostage-receives-mysterious-funeral-wreath-initial-shin-bet-investigation-suggests-iranian-agents.

[4] Benjakob, O. Iran Leaking Sensitive Information on Top Israeli Officials. Haaretz. 21 October 2024. https://www.haaretz.com/israel-news/security-aviation/2024-10-21/ty-article/.premium/iran-leaking-sensitive-information-on-top-israeli-officials/00000192-aae4-dca2-a7d2-aff41a270000.

[5] Benjakob, O. After Iran Steals Sensitive Israeli Data, Israel Tries to Censor the Internet. Haaretz. 21 August 2024. https://www.haaretz.com/israel-news/security-aviation/2024-08-21/ty-article-magazine/.premium/israels-futile-war-against-massive-iranian-hack-of-secret-data/00000191-6bd7-d1ee-afb5-6bff8a510000.

[6] Fabian, E.; Staff, T. Shin Bet: Iran targeted senior Israeli figures with over 200 cyberattacks. The Times of Israel. 2 December 2024. https://www.timesofisrael.com/shin-bet-iran-targeted-senior-israeli-figures-with-over-200-cyberattacks/.

[7] Ynet. The Purpose - Assassination: 200 Cyber Attacks by Iran Against Senior Israeli Officials Exposed. 2 December 2024. https://www.ynet.co.il/news/article/sjimfxjqyx.

[8] Fabian, E. Ex-defense minister Ya'alon was target of Hezbollah bomb attack in Tel Aviv last year. The Times of Israel. 18 September 2024. https://www.timesofisrael.com/ex-defense-minister-yaalon-was-target-of-hezbollah-bomb-attack-in-tel-aviv-last-year/.

[9] Sakellariadis, J. Iranian hackers – and hitmen – eye Trump. Politico. 19 August 2024. https://www.politico.com/newsletters/weekly-cybersecurity/2024/08/19/iranian-hackers-and-hitmen-eye-trump-00174546.

[10] Wikipedia. Assassination of Qasem Soleimani. https://en.wikipedia.org/wiki/Assassination_of_Qasem_Soleimani.

[11] Benjakob, O. Israel Struggles With Iran's Recruiting of Its Citizens for Spying. Haaretz. 31 January 2025. https://www.haaretz.com/israel-news/security-aviation/2025-01-31/ty-article/.premium/israel-struggles-with-irans-recruiting-of-its-citizens-for-spying/00000194-bd2b-d5a7-ab9d-ffbb55ca0000.

[12] Peleg, B.; Benjakob, O.; Breiner, J. Iranian networks have been active among right-wing and left-wing groups in an attempt to deepen the rift in Israel. Haaretz. 16 June 2023. https://www.haaretz.co.il/news/politics/2023-06-16/ty-article-magazine/.premium/00000188-bfbb-d2e6-a9ab-ffbf824f0000.

[13] Benjakob, O. Shin Bet: Iran used Israelis to photograph the homes of security personnel and encourage the treatment of abductees. Haaretz. 15 January 2024. https://www.haaretz.co.il/news/politics/2024-01-15/ty-article/0000018d-0e82-de9c-a3df-6ffbbed60000.

[14] Benjakob, O. Iranian Counterintelligence Operation Targeting Israeli Collaborators Exposed by Google. Haaretz. 29 August 2024. https://www.haaretz.com/israel-news/security-aviation/2024-08-29/ty-article/.premium/iranian-counter-intelligence-operation-targeting-israeli-collaborators-exposed-by-google/00000191-9f00-d453-ab9f-ff8cee220000.

[15] Benjakob, O.; Melman, Y. Personal Threats and Harassment: Iran Escalates Psychological Warfare Against Israelis. Haaretz. 18 April 2024. https://www.haaretz.com/israel-news/security-aviation/2024-04-18/ty-article/.premium/personal-threats-and-harassment-iran-escalates-psychological-warfare-against-israel/0000018e-ecc8-dbb3-a3bf-fdcdb1840000.

[16] Benjakob, O. How Iranian 'Agents' Are Trolling Israel: $20 for Graffiti, With a Bonus for Arson. Haaretz. 7 February 2025. https://www.haaretz.com/israel-news/2025-02-07/ty-article-magazine/.highlight/how-iranian-agents-are-trolling-israel-20-for-graffiti-with-a-bonus-for-arson/00000194-dd43-d6d4-a3d6-ffeb6eab0000.

[17] Breiner, J. Shin Bet to Indict Israeli Who Was Allegedly Recruited by Iran Online to Commit Acts Against State. Haaretz. 16 July 2024. https://www.haaretz.com/israel-news/2024-07-16/ty-article/.premium/shin-bet-to-indict-israeli-allegedly-recruited-by-iran-to-commit-acts-against-state/00000190-bbd9-d211-a5da-ffdbe2140000.

[18] Melman, Y. What Made an Israeli Student Work for Iranian Intelligence? Haaretz. 9 September 2024. https://www.haaretz.com/israel-news/2024-09-09/ty-article/.premium/what-made-an-israeli-student-work-for-iranian-intelligence/00000191-d656-deec-add7-de57ca1e0000.

[19] Peleg, B.; Shimoni, R.Israeli Couple Charged With Aiding Iran, Including Plotting to Assassinate Public Figure. Haaretz. 14 October 2024. https://www.haaretz.com/israel-news/2024-10-14/ty-article/.premium/israeli-couple-charged-with-aiding-iran-including-plotting-to-assassinate-public-figure/00000192-8a9f-d569-a3be-debfabb30000.

[20] Melman, Y. Analysis | Israeli Jews Very Rarely Agreed to Spy on Behalf of Israel's Worst Enemies. What's Changed? Haaretz. 23 October 2024. https://www.haaretz.com/israel-news/2024-10-23/ty-article/.premium/israeli-jews-very-rarely-agreed-to-spy-on-behalf-of-israels-worst-enemies-what-changed/00000192-b598-d243-a5db-fdf92cee0000.

[21] Breiner, J.; Maanit, C. Shin Bet, Police Arrest Israeli Man Allegedly Recruited by Iran to Carry Out Assassination. Haaretz. 16 October 2024. https://www.haaretz.com/israel-news/2024-10-16/ty-article/.premium/shin-bet-israeli-police-arrest-man-allegedly-planning-assassination-for-iran/00000192-940c-dbf3-a1be-dd3f69930000.

[22] Check Point. Iranian Spear-Phishing Operation Targets Former Israeli and US High-Ranking Officials. 14 June 2022. https://research.checkpoint.com/2022/check-point-research-exposes-an-iranian-phishing-campaign-targeting-former-israeli-foreign-minister-former-us-ambassador-idf-general-and-defense-industry-executives/.

[23] Benjakob, O. Shin Bet: We have thwarted more than 80 attempts at Iranian cyberattacks against Israelis, including senior security officials. Haaretz. 29 May 2025. https://www.haaretz.co.il/news/politics/2025-05-29/ty-article/00000197-1bb2-df22-a9d7-9ff2c2670000.

[24] Benjakob, O. Thousands of Israeli Gun Owners Exposed in Iranian Hack-and-leak Operation. Haaretz. 9 March 2025. https://www.haaretz.com/israel-news/security-aviation/2025-03-09/ty-article-magazine/.premium/thousands-of-israeli-gun-owners-exposed-in-iranian-hack-and-leak-operation/00000195-6625-d4c2-a5f5-76af57cd0000.

[25] Watts, C. Iran accelerates cyber ops against Israel from chaotic start. Microsoft. 6 February 2024. https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/.

[26] Ohana, L.; Glickman, E. Serious espionage case: Israelis will be charged with photographing bases that were targets in the Iranian attack. Ynet. 21 October 2024. https://www.ynet.co.il/news/article/hjzhw9xgyx.

[27] Wikipedia. GRU Unit 29155. https://en.wikipedia.org/wiki/GRU_Unit_29155.

[28] CISA. Russian Military Cyber Actors Target US and Global Critical Infrastructure. 5 September 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a.

[29] National Cyber Security Centre. UK and allies uncover Russian military unit carrying out cyber attacks and digital sabotage for the first time. https://www.ncsc.gov.uk/news/uk-allies-uncover-russian-military-carrying-out-cyber-attacks-digital-sabotage.

[30] El-Hai, L. Documenting strategic bases and sites: Two young men arrested on suspicion of spying for Iran. Ynet. 23 June 2025. https://www.ynet.co.il/news/article/sk6jayl4lx.

[31] Solomon, E. Israeli Sentenced to 10 Years in Prison for Plotting With Iran to Assassinate Top Israeli Officials. Haaretz. 29 April 2025. https://www.haaretz.com/israel-news/2025-04-29/ty-article/israeli-sentenced-to-10-years-in-prison-for-iran-plot-to-kill-top-israeli-officials/00000196-8123-d9ad-a19e-c5b7dad90000.

[32] Saul, J. Israel arrests seven Jerusalem residents over alleged Iran assassination plot. Reuters. 22 October 2024. https://www.reuters.com/world/middle-east/israel-arrests-seven-jerusalem-residents-over-alleged-iran-assassination-plot-2024-10-22/.

[33] Singer, R. Inside the 'Spy Wing' for Israelis Suspected of Spying for Iran. Shomrim. 26 June 2025. https://www.shomrim.news/eng/inside-the-spy-wing.

[34] Curiel, I. The technician accused of offering Israel's nuclear secrets to Iran. Ynet. 3 February 2025. https://www.ynetnews.com/article/h1npkgzi1e.

[35] Gabay, Y. Carried an explosive device: Israelis spied for Iran - and installed cameras near the defense minister's house. Kikar. 20 May 2025. https://www.kikar.co.il/security-news/swk2fu.

[36] Ravid, O. 13-year-old from MTA arrested: "Suspected of carrying out missions for Iran, asked to photograph Iron Dome". N12. 20 June 2025. https://www.mako.co.il/news-military/f239747af17c5910/Article-fdac645ad295791027.htm.

[37] Staff, T. Alleged spy for Iran placed powerful explosives near defense minister's home – report. The Times of Israel. 29 June 2025. https://www.timesofisrael.com/man-suspected-of-spying-for-iran-planted-explosives-near-defense-ministers-home-report/.

[38] News - Israel Broadcasting Corporation. Exclusive documentation: The young men from Nesher suspected of spying for Iran in action. YouTube. https://www.youtube.com/watch?v=Pdcmztw5Fp0.