Research Forum

Flag of Hezbollah

Intelligence Agents in Israel: Hezbollah’s Modus Operandi

Gil Riza
Independent Researcher

Terrorist organizations operate intelligence units that aim primarily to obtain valuable information about their adversaries, in order to plan terrorist attacks and gain counterintelligence, and thereby reduce the intelligence gathered by the adversary. This article presents a study that in the limits of an empirical framework analyzes Hezbollah’s modus operandi of intelligence agents in Israel. The purpose of the study, which analyzes quantitative and qualitative content from 21 rulings against 41 Israeli men and women who were accused of spying for Hezbollah in Israel between 2000 and 2021, is to expose the methods of operation of Hezbollah’s agents in Israel and to shed light on the status of human intelligence (HUMINT) in Hezbollah’s intelligence efforts. The activity of most of the agents was exposed by Israeli counterintelligence within a short amount of time, and their operation did not cause significant damage to Israel.

Keywords: Hezbollah, intelligence, HUMINT, counterintelligence, espionage, agents, ideology, reward, psychological-mental

Introduction

States engage in intelligence and to this end establish national intelligence agencies, and over time terrorist organizations have likewise developed intelligence capabilities, including human intelligence (HUMINT) capabilities. In the areas in which they operate, terrorist organizations, like states, build intelligence capabilities for the purposes of internal security, preventive capabilities against the activity of adversary intelligence organizations, and intelligence for operational, tactical, and strategic needs for carrying out various kinds of terrorism (Gentry, 2016). Many weaknesses are apparent in terrorist organizations' use of intelligence—mainly vis-à-vis the state adversary—such as a lack of resources, the high level of effectiveness of the state's counterintelligence (Tsichritzis, 2015), and problems that stem from the nature of terrorist organizations and their organizational culture. Sometimes organizations do not permit freedom of expression and thought, and make it difficult to carry out high-quality analysis of intelligence products (Bitton, 2019). However, through concerted efforts terrorist organizations have succeeded in developing a variety of intelligence capabilities that include operation of agents, observations, and surveillance, which have led to successful terrorist attacks (Riedel, 2011).

Over the years Hezbollah has succeeded in recruiting intelligence agents in Israel that provided the organization with diverse information about Israel.

Over the years Hezbollah has succeeded in recruiting intelligence agents in Israel that provided the organization with diverse information about Israel, but the damage caused to Israel was not always clear; rather, it was mainly potential damage that could be used in the next armed conflict with Hezbollah. Residents of Israel that chose to engage in espionage for Hezbollah usually did so out of monetary and ideological motivations (Kulick, 2009). While occasionally incidents of espionage for Hezbollah are exposed in the Israeli media, research on the phenomenon of Israeli agents who choose to help Hezbollah with intelligence is relatively limited. Kulick's study (2009), which is considered one of the earliest studies on the operation of Israeli agents for Hezbollah's intelligence needs, is an important landmark. This study found inter alia that Hezbollah expanded the recruitment of agents beyond just drug deals, and showed that Hezbollah began to extend its intelligence gathering in all parts of the State of Israel and not just on the northern border.

However, Kulick's study is relatively dated and does not include many incidents of espionage that came to light over the years. It lacks information about the acts of espionage, such as the duration of the agents' activity; new methods of recruitment (e.g., on social networks on the internet); and demographic characteristics, including the age and employment of the agents. Kulick's study mainly describes several famous incidents of espionage, such as a lieutenant-colonel in the IDF who engaged in drug trafficking and espionage, large drug networks that operated in cooperation with Hezbollah, and university students who studied abroad and met with Hezbollah operatives there.

The purpose of the study below is to present the modus operandi of Hezbollah agents in Israel and from analysis of the findings understand the nature of Hezbollah human intelligence, based on 21 legal rulings on Israeli residents who engaged in espionage for Hezbollah and were convicted in Israeli courts between 2000 and 2021. The empirical and qualitative findings reveal how the agents were recruited and operated, the characteristics of the agents, the motivations for carrying out the acts of espionage, and the duration of the agents' activity, along with an explanation of the preventive processes by the Israel

Security Agency (ISA) as part of its official role—preventing espionage in Israel.

The first section of the article presents the topic of espionage, intelligence, and the terrorist organizations. It includes definitions of espionage and intelligence, the motivations for espionage, the importance of intelligence for terrorist organizations, and the intelligence challenges of the terrorist organizations, along with a short description of the operation of Hezbollah's intelligence against Israel. This section is followed by presentation of research methods and methodology, criteria for analysis, and the population studied. The findings of the empirical-qualitative research that arose from analyzing the case studies (41 defendants) are presented next, followed by the article's principal conclusions.

Espionage, Intelligence, and Terrorist Organizations

Definitions

According to Israeli law, the definition of a person engaged in espionage is: "(a)Someone who has conveyed information and intended to harm the state's security…(b)Someone who has obtained, gathered, prepared, written, or withheld information and intended to harm the state's security" (Penal Law 1977, section 112). In other words, espionage is an act of gathering information in practice and transferring it to an unauthorized person, with the intent of harming the state's security.

The definition of one who conveys information to an enemy is: "Someone who knowingly conveyed information to or for an enemy…; the information could benefit the enemy…; in so doing intended to harm the state's security…; through negligence caused information to be conveyed to or for an enemy that could benefit it" (Penal Law 1977, section 111). In other words, conveying information to an enemy, unlike espionage, does not necessarily include only an intention to harm the state, and the act can also be carried out due to negligence. This interpretation likewise allows an understanding of the definition of intelligence, which includes information obtained through the action of espionage.

Motivations for Espionage

Espionage by citizens against their country or the organization with which the individual is affiliated is to a large extent based on four main motivations: ideology, when the agent morally and ideologically opposes the regime or country and is willing to spy as an expression of this opposition; material, medical, symbolic, or other reward, which the agent seeks to obtain by agreeing to spy; revenge, when the agent seeks to take revenge on his country for a negative action or occasion that he experienced; and a psychological-mental motivation based on a particular aspect of his personality (Lillbacka, 2017; Thompson, 2014). Even though historically these motivations were identified with cases of espionage against states, it has been posited that agents' motivations for acting in favor of the interests of terrorist organizations and providing them with intelligence about the state or about the organization that they themselves work in are based on similar motivations, but with an emphasis on ideology and monetary reward (ISA, 2014; Harber, 2009).

The ideological motivation for espionage is considered one of the strongest motivations, because it involves the agent's views and beliefs that he is doing the right thing for a cause that he believes in and wants to advance. The ideological agent, even if it involves treason against his nation-state, still sees the mission of espionage as a moral obligation (Thompson, 2014).

A second motivation, reward, can be monetary or its equivalent or other benefits. The motivation of reward is based on the view that the life circumstances of the agent obligate him or have habituated him to obtain the necessary reward. For example, a monetary motivation can be based on a debt that the agent faces, or difficulty supporting himself and his family. Intelligence organizations worldwide invest sums of money, equivalent rewards, and benefits in order convince agents to work for them and provide them with information (Lillbacka, 2017).

Vengeance is another motivation that constitutes a basis for the operation of agents. Sometimes people act against their country or against the organization they are members of out of a sense of revenge and resentment about a process that they experienced on the part of the country or organization (Thompson, 2014).

The fourth motivation is psychological-mental, which refers to the character and personality structure of the individual (Thompson, 2014). For example, someone could be worried about personal problems or have a need to appease or help others; have ego problems, personality disorders, antisocial behaviors, psychopathic problems, mental disability; display narcissism or immaturity; or harbor a strong need for gratification. Sometimes deep personal needs based on emotions push the person to engage in espionage against his country and his society (Lillbacka, 2017). Another approach notes that sometimes the motivation for espionage is not necessarily based on a single factor but rather a convergence of factors such as an ideological motivation and reward, a psychological motivation joined with revenge, or other combinations (Thompson, 2014).

The ideological motivation is often defined as the strongest motivation for a person to spy, because it is a motivation based on a sense of moral obligation in which a person feels a real need to engage in espionage over time. The monetary motivation, despite being very common (Lillbacka, 2017), is often considered a less stable and perhaps short-term motivation, because the agent sometimes believes that the scope of potential damage of the espionage and the fear of being caught outweigh the advantages from the payment that he receives. In addition, the agent's operators do not always agree to meet his monetary demands, and as a result, a crisis can arise in the operation of the agent (Lillbacka, 2017; Thompson, 2014).

Similarly, the motivation of vengeance is often short term, because the agent could end his espionage activity when he concludes that he has fulfilled his desire for revenge. The psychological-mental motivation is considered a complex motivation in the operation of the agent and potentially unstable over time, because the motivation is not necessarily immediate. It could emerge and inundate the agent over time or stem from a one-time problem that could pass after an undefined period, and sometimes it is a prolonged mental-psychological problem (Lillbacka, 2017). The motivations that encourage people to spy on their country or on other entities are used by state and non-state intelligence agencies when recruiting agents into their ranks.

The Use of Intelligence by Terrorist Organizations

From the state's perspective, the use of intelligence aims mainly to fulfill four central objectives: internal security for protecting the country from violence and subversion; overt, covert, or secret tactical action; decision making and policy shaping; and prevention of foreign intelligence activities. Similarly, non-state organizations such as non-governmental institutions, trade organizations, and terrorist organizations also utilize intelligence for the purpose of fulfilling these objectives (Gentry, 2016).

Non-state organizations are organizations that are not state or governmental, even though they are sometimes created by states. There are various kinds of non-state organizations, from social organizations to environmental organizations to belligerent military organizations such as terrorist organizations. Non-state organizations employ intelligence capabilities to fulfill the same intelligence objectives that states seek to fulfill. However, when focusing on terrorist organizations, the common approach is that these organizations employ intelligence capabilities mainly for the purpose of planning offensive actions and for the sake of counterintelligence, which aims to protect the organization from penetration by adversaries (Gentry, 2016).

Terrorist organizations employ intelligence in an organized and calculated manner similar to the way intelligence is employed by states. Intelligence gathering methods include obtaining information through technological means and with the help of people. Technological intelligence includes signals intelligence (SIGINT), which is based on intercepting electronic communication such as phone calls and computer communication; visual intelligence (VISINT), which is based on pictures from satellites or aircraft and other photographs; and open source intelligence (OSINT), which is based in part on technologies such as the internet and computer databases that are open to the general public, as well as the use of tools that are not technological such as books, maps, news media, and more. Alongside technological intelligence, there is human intelligence (HUMINT), which is the focus of this article. Human intelligence is based on gathering intelligence that is produced from evidence and interpretations by people, or from people who provide the information on their own in raw form such as documents. This intelligence can sometimes be less reliable, but it can provide insights about facts, events, and processes that SIGINT and VISINT are unable to explain (Gentry, 2016).

Through HUMINT and the use of technologies, terrorist organizations have on several occasions achieved major successes against adversary countries and have even caused damage to highly reputable intelligence organizations. For example, in 2009 al-Qaeda succeeded in operating a double agent against the CIA. The agent succeeded in spying on the CIA in Afghanistan, identifying the organization's agents, penetrating secure CIA buildings in Afghanistan, and killing American intelligence officers. Another example of the quality of intelligence of terrorist organizations is the attack that took place in Mumbai, India, in 2008. The attack, carried out by ten terrorists from the organization Lashkar-e-Taiba, caused hundreds of deaths and injuries and the siege of a city of 14 million residents. Considerable intelligence was collected prior to the attack, including assessment of the security arrangements on the maritime border between India and Pakistan, security arrangements in the building targeted in the attack, surveillance of individuals, and identification of potential targets prior to the attack. The intelligence gathering process lasted many months, and only at its end was the appropriate operational infrastructure formed for carrying out the attack (Riedel, 2011).

Through HUMINT and the use of technologies, terrorist organizations have on several occasions achieved major successes against adversary countries and have even caused damage to highly reputable intelligence organizations.

Despite the successes and the similarity in intelligence gathering methods between states and terrorist organizations, there are substantial gaps between the intelligence of a state and that of a terrorist organization. For example, legal, political, and national limitations that apply to states in the use of intelligence do not apply to terrorist organizations (e.g., issues of individual rights or a state decision not to spy on a certain country). Terrorist organizations do not see themselves as limited in these areas, and from their perspective they are free to spy on any target that in their opinion is worth following (Harber, 2009).

Terrorist organizations do not enjoy the same human, technological, and budgetary resources that states have. The latter can invest enormous resources in recruiting quality intelligence personnel, training agents and personnel at a high level, developing technologies, and establishing infrastructure for gathering and analyzing intelligence. Terrorist organizations, in contrast, are hard pressed to recruit significant amounts of financial capital to enable them to develop large-scale espionage and intelligence infrastructure that would compare to the means at the disposal of states. Even large terrorist organizations and those that have proved impressive operational capabilities in the past, such as Hezbollah and al-Qaeda, have always been characterized by relatively scarce resources compared to the intelligence units of states, and they have had difficulty developing complex espionage and intelligence capabilities with quality manpower and sophisticated equipment (Harber, 2009).

But despite the gaps, terrorist organizations nonetheless succeed in establishing fairly high-quality intelligence infrastructure for themselves. They can recruit high-quality agents by encouraging ideological motivations and the desire for revenge. A shared religious identity between the organizations and potential recruits, common ideological foundations, and a shared sense of hatred toward enemies can be fertile ground for recruiting human capital to terrorist organizations that have difficulty recruiting agents based on rewards (Tsichritzis, 2015). Terrorist organizations cope with technology challenges such as high costs of technological surveillance products or the complexity of operating them with the help of relatively cheap and available technological alternatives. The internet market offers a variety of cyber services and technological tools that can be acquired easily and often cheaply. Furthermore, terrorist organizations can engage in cyber fraud, including stealing money and intercepting credit cards—actions that can expand their financial capital (Siboni et al., 2013). However, even the cyber capabilities of a terrorist organization require quality human capital, and so a terrorist organization will generally have to recruit people who are highly educated and have advanced skills, and for this reason the limitation of resources was and is a fundamental problem for it.

Another challenge facing terrorist organizations in attempting to gather and produce intelligence relates to their organizational culture. Terrorist organizations are usually based on authoritarian leadership that restricts stances that oppose that of the leader, and requires the organization's member to act in accordance with the judgment and opinions of the leader. This is an important limitation because intelligence analysis requires freedom of thought and freedom of expression, which enable casting doubts on the products of intelligence, stimulating new ideas, and analyzing products and the adversary's behaviors in a free and diverse manner. Therefore, decisions made based on mistaken intelligence analysis could be fatal to the organization's integrity (Bitton, 2019).

The problem of intelligence cooperation with other organizations is also considered a challenge for terrorist organizations. While states tend to cooperate with their allies regarding intelligence and thereby broaden the intelligence information at their disposal, terrorist organizations tend to limit their cooperation with other terrorist organizations and actors due to their compartmentalization and concern about penetration of the organization and rivalry between organizations (Gentry, 2016). Nonetheless, terrorist organizations sometimes tend to cooperate with one another based on shared hostility toward an adversary, and this in turn can also help intelligence cooperation (Tsichritzis, 2015).

Hezbollah's Use of Intelligence against Israel

Hezbollah's modus operandi, which shows that intelligence gathering is an important element in the organization's activity, is based on seven principal methods: gathering intelligence for operational activity; counterintelligence to reduce the organization's exposure to adversaries; diplomatic, educational, and business activity to conceal the organization's terrorist activity; penetration of groups that oppose the organization; logistical planning for future attacks; recruitment of operatives; and assassination of organization adversaries and opponents (Levitt, 2020; Pop & Silber, 2021).

Hezbollah cultivates its intelligence capabilities in ongoing fashion. These include technological capabilities such as cyber, aircraft for intelligence gathering, wiretaps, interception of communication and more, as well as human intelligence capabilities of recruiting agents within Israeli territory (Michael & Dostri, 2018; Kulick, 2009). Hezbollah began to develop organized intelligence capabilities mainly during the 1990s, after the end of the Lebanese Civil War in 1989 (the Taif Agreement). At first the organization established several intelligence units such as a counterintelligence unit; a security and military intelligence unit for operational networks in Lebanon; and a security and intelligence unit in foreign countries such as Unit 910, which engages in operations and intelligence in foreign countries including recruiting intelligence agents, gathering intelligence before an operation, and conducting operational activities (Wege, 2016).

Over the years, as Hezbollah's operational capabilities evolved, the operational units that also engage in intelligence expanded. At first, it was Unit 1800, which engages in operational activity and intelligence in countries neighboring Israel (including among Palestinians). Out of this unit, early in the 2000s Unit 133 was established, which aims to wage attacks within Israel and to gather intelligence prior to operations (Buhbut, 2016; Wege, 2016). These intelligence units engaged in gathering intelligence through both technological and human capabilities. An assessment of Hezbollah's intelligence activity describes how the organization employs intelligence mainly for the purpose of preparing for actions and as counterintelligence to prevent the adversary's penetration into the organization (Shapir, 2017).

Even though some of Hezbollah's units include a combination of intelligence and operational activities, the organization tends to separate different professional areas and is not necessarily quick to assign its fighters several simultaneous roles, but rather makes sure to assign the right people to the right unit for them and for Hezbollah. This management is reminiscent of a military practice in which the system is divided into different organizations and different position holders. In addition, Hezbollah tends to invest heavily in the professional training of fighters in operational units such as training on constructing explosives and operating weapons, and only operatives with promising potential quickly integrate in these units. In contrast, the field of intelligence is sometimes assigned to new recruits who have not yet proven themselves, or put in the hands of operatives who are not intended for combat roles (Levitt, 2020; Pop & Silber, 2021).

In the field of technological intelligence gathering, the Shiite organization enjoys technological cooperation with Iran, which enables it to improve its offensive cyber and intelligence gathering capabilities (Lt. Col. H. et al., 2021; Siboni & Kronenfeld, 2015). The easy access to drones on the free market in terms of price, model, and simple operation has made them a readily available and convenient intelligence tool for terrorist organizations, including Hezbollah. These drones have offensive and intelligence gathering capabilities using simple cameras (State Comptroller, 2021). Hezbollah also engages in gathering open source information from both the internet and electronic databases and from various information manuals and books that are available on the free market (Kulick, 2009). It has stationed observation towers close to the border region with Israel (despite Security Council Resolution 1701 from 2006 following the Second Lebanon War, which prohibits the stationing of military forces in South Lebanon except by the Lebanese Army) and uses them under ridiculous pretexts such as observation towers for the protection of nature, in which they place observers in civilian guise ("IDF Reveals," 2018).

Alongside these methods, Hezbollah engages in the operation of intelligence agents within a target country, and has succeeded in recruiting and operating many agents in Israel and in other countries worldwide. Hezbollah's modus operandi in operating agents is often based on the use of local civilians who are not Lebanese. Because the source of Hezbollah's activity is in Lebanon, Lebanese citizens in foreign countries could in various cases arouse natural suspicion on the part of the counterintelligence units of the foreign country. Therefore, in many cases Hezbollah instead tends to rely on local populations that are not Lebanese for the purpose of espionage activities and other operational activities. These residents provide excellent cover for the organization because they are local citizens who are familiar with the attitudes in the country and enjoy freedom of movement within their country and in access to and from it ("Hezbollah Activity," 2014; Levitt, 2020; Pop & Silber, 2021).

The information that the agents in Israel have supplied to Hezbollah is diverse, including the location of critical civilian and military infrastructure, orders of battle, border points, and information on IDF weapons.

The recruitment of espionage agents in Israel for Hezbollah is associated mainly with the Arab population in Israel, including former Member of Knesset Azmi Bishara, who was suspected of supplying various intelligence information to Hezbollah during the Second Lebanon War in 2006; an IDF officer of Bedouin origin at the rank of lieutenant colonel who supplied intelligence information to Hezbollah early in the 2000s; and ordinary residents in various areas of Israel (Kulick, 2009). However, there are not only agents from minority Arab or Bedouin groups, but also Jewish agents who have supplied intelligence information to Hezbollah as part of drug deals (see below, criminal case 03/36 State of Israel vs. Said ben Jamil Kahmouz).

The information that the agents in Israel have supplied to Hezbollah is diverse, including the location of critical civilian and military infrastructure, orders of battle, border points, and information on IDF weapons. In addition, Hezbollah has sought to gather social information on various issues, including political rivalries, government systems, social struggles, social trends, and more, in order to identify strengths and weaknesses of Israeli society, military vulnerabilities, and future targets, and even in order to understand the mood in the country (Zeitoun et al., 2021; Kulick, 2009). The Israeli agents were recruited into Hezbollah service based on various motivations, including ideological and economic reasons (Kulick, 2009).

The damage caused due to the operation of agents in Israel is not only direct damage. There is evidence that Hezbollah has operated agents for the purpose of terrorist attacks, but they were caught before the attack or injured in the process of preparing for the attack. Agents have provided a range of intelligence information to Hezbollah, including military and civilian information, which could be used for attacks in the future. For example, information provided to Hezbollah on the locations where missiles have fallen in Israel can be used by the organization to correct the ranging of missiles—which, in the next conflict with Hezbollah, could increase the number of casualties and the extent of the damage to infrastructure in Israel, and thus harm Israel's resilience (Kulick, 2009).

While over the years terrorist organizations operating against Israel have succeeded in recruiting various agents, there are almost no studies on the recruitment and operation of Israeli agents and intelligence gathering for terrorist organizations. There are two possible reasons for this: the first is that the primary and clear interest is in intelligence organizations that operate under the auspices of states and in their framework; the second reason is the later interest of states in intelligence on terrorist organizations following the global war against terrorism (declared by the United States after the September 11 terrorist attacks) and the increasing and joint involvement of states in the fight against terrorism. Therefore, the rise in the publication of studies on the activity of terrorist organizations and their intelligence units began at a relatively late stage (Strachan-Morris, 2019).

In the Israeli context, Kulick's study (2009) is apparently the only one in the field that focused on the operation of Israeli agents for the purpose of intelligence for Hezbollah. It is considered a unique study that describes several cases of Israeli agents that operated in the service of Hezbollah's intelligence. Prominent and important findings in Kulick's study revealed that Hezbollah expanded its attempts to gather intelligence in Israel, and not only as part of drug deals. The organization broadened and diversified its intelligence targets beyond Israel's northern border, and today gathers extensive information about Israel and the deployment of military forces throughout the country and engages in identifying strategic targets. This suggests that in a future war, Hezbollah will try to fire missiles toward distant and strategic targets. In addition, Hezbollah has increased its interest in Israeli society in order to understand its strengths and weaknesses and exploit them in the next conflict.

Nevertheless, despite its importance and uniqueness, Kulick's study is considered dated and lacks important information, such as the duration of the espionage activity, demographic characteristics of the agents, in-depth assessment of the impacts of the damage that it caused Israel, and more, from which many insights can be derived regarding the modes of operation of Israeli agents by Hezbollah. In addition, there are occasional reports in the media about the exposure of agents in Israel who operated for Hezbollah. However, these important reports do not describe trends and changes over time, but rather coverage of individual incidents. The current study seeks to provide a more comprehensive and current examination of the modes of operation of Israeli agents by Hezbollah.

Methodology

The study is based on quantitative and qualitative content from rulings that focus on the prosecution of Israeli agents that Hezbollah operated in Israel. The list of rulings appears in the Appendix below. Some of the rulings include more than one defendant, but in the study each agent is examined individually. For the purpose of examining relevant rulings, the Pador legal database was used. Relevant rulings were searched and identified by filtering according to the combination of keywords "Hezbollah" and "Lebanon," as well as "espionage" and "conveying information to an enemy," which appear in Penal Law 1977, which was the basis for charging the agents in Israel.

The use of rulings alone stems from the extensive detail of the indictment described in the ruling, the sides' respective arguments, and the judge's decision, which together describe details at length that are essential to the study, including the age of the defendants, the period of their activity, the types of charges, motivations, and more. The study assumes that not all cases of the operation of intelligence agents by Hezbollah in Israel have been publicized in the legal databases open to the public. In some cases, it is known that a gag order was placed on the indictments, although reports about the incident appeared in the media, and in other cases the defendants were in administrative detention and no indictment was filed against them yet. Consequently, the premise of the study is that any figure that is received about the extent of operation of Hezbollah intelligence agents in Israel does not reflect the precise number of cases known in practice.

The study focuses only on rulings issued between the years 2000 and 2021. The opening date relates to Israel's withdrawal from Lebanon in 2000, at which point Hezbollah had to change the modus operandi of its agents against Israel and operate them from within the borders of

Israel and not from the security zone that the IDF maintained until its withdrawal. With respect to the population of the study, the focus was only on Israeli agents—Israeli residents or citizens living permanently or sporadically in Israel and who spied for Hezbollah (but it is possible that they also engaged in other activities such as smuggling drugs and weapons and carrying out terrorist attacks).

To focus the study, an initial reading of the rulings was carried out in order to identify several criteria that recurred in the indictments. The criteria for examination were: the motivations for spying, the charges of espionage as they appear in the rulings, demographic characteristics (gender, age, profession, and residence), duration of the espionage, way of meeting with the operator, methods and means of espionage, and level of damage caused to Israel. Prior reading of the rulings reveals that they lack complete details of the demographic information of the agents or of the rewards that some of them received, and so while the demographic information and kinds of motivations were examined in the study, the information on them is not necessarily complete. Based on the filters presented above, 21 relevant rulings were identified, which included 41 defendants.

Findings

Recruitment

Table 1 presents the year of recruitment of the agents but not the year of their exposure. Some of the agents acted together and joint indictments were filed against them. An analysis of the publicly available rulings reveals that from 2000 to 2021, Hezbollah worked continuously over time to recruit and operate agents and operated 41 Israeli agents who supplied the organization with intelligence information. A year that doesn't appear in the table is one in which the recruitment of an Israeli agent was not identified, but this does not mean that in any such year no Hezbollah agents were recruited and operated in Israel.

Table 1. Recruitment year

Year of recruitment	Number of agents
2000	5
2001	10
2002	4
2003	3
2005	1
2006	3
2007	2
2008	1
2009	1
2010	7
2012	1
2015	1
2018	1
2019	1

Recruitment Methods

The figures on the extent of the recruitment of agents raise key questions: who initiated the recruitment, how were the agents recruited, and where did the recruitment take place. The figures show that the initial initiative for recruitment, meaning who initiated the first contact for the purpose of recruitment, came mostly from the Israeli agents. Out of 21 indictments, about 10 indicated that the defendants were those who had made the initial contact with Hezbollah and offered their services to the organization (Table 2). Enlistment in Hezbollah took place in a variety of forms. Out of the ten enlistment initiatives on the part of the defendants, half were related to drug trafficking. The defendants made contact with criminal elements in Israel (who knew drug traffickers in Lebanon) or with Lebanese drug traffickers in order to smuggle drugs into Israel, and their connection with Hezbollah developed out of this activity.

Table 2. Enlistment initiative

Initiated enlistment to Hezbollah	Number
From the defendants (the Israeli agents)	10
From Hezbollah	7
Unknown	4

When Hezbollah was the side that initiated the recruitment of the agents, there were at least five cases in which the potential Israeli agent was abroad for the purpose of study, educational-social activity, pilgrimage to Mecca, or family vacation, and Hezbollah made contact with them during their stay in a foreign country. Only in one case did Hezbollah proactively contact defendants on social media, after the organization identified a potential recruit from his statements on the internet. Of the initiatives for recruitment, only in three cases did the recruitment take place over the internet (once at Hezbollah's initiative and twice at the agents' initiative). The use of the internet included social media such as Facebook and Twitter, where groups that serve Hezbollah's interests are managed, or even on the al-Manar website, which is identified with Hezbollah.

In the case of a spy ring, which was usually identified as part of drug deals, the process of recruitment by Hezbollah included at first a meeting of the head of the spy ring (sometimes with another partner) with Hezbollah operatives, and afterwards the network grew through the "bring a friend" method on the part of the agents in Israel. The recruitment of partners using this method was also carried out by Hezbollah, and in at least three cases Hezbollah tried to encourage the agent to attempt to recruit additional acquaintances to the organization and encouraged the agent to provide Hezbollah with details on potential recruits. Whether the recruitment occurred over the internet, as part of drug trafficking, or as part of time spent abroad, in most cases ultimately direct face-to-face contact was made between the agent and the Hezbollah operator (in the case of a spy ring, only one or two representatives from the spy ring met with the Hezbollah operators). During these meetings it was made clear to the recruits that the person standing in front of them was operating in the service of Hezbollah.

Contact

The operation of the agents and the physical meeting between the agent and his operator usually took place along the border between Israel and Lebanon, although on many occasions recruitment and operation of agents also took place abroad, in Arab and European countries (Table 3). The frequent meetings between agents and operators on the border could hint at direct and possible crossing between Israel and Lebanon. The accessibility of the agents to Arab countries that do not have official relations with Israel was carried out through a third party—Egypt, Jordan, or another country, to which the agents could move freely. Some even visited several countries with their operators. Some of the meetings took place in random frameworks, for example as part of studies abroad, educational delegations abroad, or pilgrimages to Mecca in Saudi Arabia, and in other cases the agents flew abroad to meet their operators. In all the meetings between the Israeli agents and Hezbollah personnel, no case was identified in which the meeting took place within Israeli territory.

Table 3. Contact with Hezbollah personnel

Meeting place	Number of agents
On the border with Lebanon	19
Unknown	6
Lebanon via the village of Ghajar	6
Lebanon	3
Denmark	2
Jordan	2
Turkey	2
Germany	1
Morocco	1
Syria	1
Saudi Arabia	1
Poland	1

Duration of Activity

The vast majority of the agents operated from several months to a full year until they were exposed (Table 4). Other agents operated continuously or on and off for several years. One agent who operated for close to six years was in fact a medical student in Germany who lived in Israel and Germany. Meeting with the agents abroad, the distance from Israel and the various visits to Israel made it difficult for the Israeli intelligence agencies to identify this activity early. However, most of the agents were identified within a few months, and some were even identified before they had managed to fulfill the demands of their operators.

Table 4. Duration of activity until exposure

Duration of the agents' activity (in years)	Number of agents
Up to one year	24
One	5
Two	6
Three	0
Four	3
Five	2
Six	1

The fact that most of the agents in Israel were exposed within a short amount of time raises a basic question about the quality of Israel's counterintelligence and the quality of the agents that Hezbollah operated. While this study does not discuss Israel's counterintelligence, different studies presented in the literature emphasize the gaps between the forces and resources at the disposal of the state that enable it to establish high-level counterintelligence infrastructure against its enemies, while non-state actors suffer from a lack of resources and have difficulty with the optimal recruitment and training of agents (Harber, 2009; Tsichritzis, 2015).

On the other hand, the quality and skills of Hezbollah's agents, characterized by a wide range of ages and diverse professional skills, should not be underestimated. Some agents were quality and professional agents with skills they acquired in the IDF or in foreign training abroad, while others did not necessarily display an understanding of espionage and did not understand in depth the significance of the espionage activity that they carried out. Hezbollah's modus operandi with Israeli agents provide the organization with convenient coverage of agents in Israel and the operation of agents from various population groups, but sometimes the lack of professionalism of the agents led to mistakes that caused their exposure, especially due to the clear superiority of Israeli counterintelligence by the ISA (Buhbut, 2015).

Demographics

Demographic information on the defendants was not presented in all the rulings. According to the information available, the vast majority of the agents were men of Arab descent, but Hezbollah did not hesitate also to use women as intelligence agents in Israel (Table 5). Four women were recruited in 2001, 2002, 2015, and 2019. Of the women, three were single and in their 20s when they were exposed, and a fourth woman (of Jewish descent) was a romantic partner of one of the defendants. In contrast, the men included single men and married men with children, and there was a wide range of ages, from 20 to 50. Most of those charged with espionage were from the north of Israel or the Galilee, but several cases were also identified from the Jerusalem area and the center of Israel. Some of the defendants held public positions and included a member of Knesset, military personnel, and workers in national institutions such as the National Library and medical institutions. The professional/occupational characteristic indicated that the agents enjoyed occupational/professional diversity in their private lives.

Table 5. Demographic information

Demographic information	Figures
Ethnic background	Arabs: 39; Jews: 2 (1 man and 1 woman)
Gender	Men: 37; women: 4
Age	20-50
Professions/ Occupations	*Public sector*: 5 military personnel, including an IDF officer at the rank of lieutenant-colonel, soldiers in regular service, and trackers. A doctor, a member of Knesset, employee of the National Library, the secretary of a school, and a college teacher. *Private sector*: University students (medicine, nursing, and law), kibbutz employees, a car mechanic, a worker at a home for autistic people, worker at a bakery, and workers at odd jobs.
Residence	The majority of the agents came from the north—the village of Ghajar on the Israel-Lebanon border, and the Galilee; some from the Jerusalem area and the center. The two Jewish agents lived in Kiryat Shmona.

Motivation

Figures on the motivations for spying were identified according to the judges' decisions in the rulings after the charges, reviews by the probation board, and defense positions were presented. Most of the agents acted out of a monetary motivation, either as a principal motivation or in combination with a secondary motivation (Table 6). The monetary motivation was identified mainly in men (except in the case of the female agent of Jewish descent); some acted out of financial distress and others out of a desire to increase their income. Most of the rulings did not explicitly list the extent of the monetary reward given to Hezbollah's agents in Israel, but only an accusation that the espionage was carried out on a monetary basis. When the espionage was part of a drug deal, the reward given to the agent was estimated to be in the thousands of shekels as part of the deal.

The various figures that were identified regarding the extent of the monetary rewards show that the scope of a single drug deal is generally estimated at between $4,000 and $10,000 (criminal case 03/36, from 02/3; various requests 001009/04). Sometimes agents carried out several drug deals for Hezbollah, and thus the total amount of money received is estimated in the tens of thousands of dollars. In one case in 2003, in which a spy ring was operated with three agents that engaged in both drug trafficking and espionage, the total amount of capital was estimated at approximately 80,000 NIS—the highest amount that was identified in all the rulings (various requests 001009/04).

In contrast, in a few cases in which there was a monetary reward that was not part of a drug deal and the amount was made public, the reward was usually estimated to be a few hundred dollars. For example, in four rulings, there was an amount between $300 and $650 (serious criminal case 652/09; serious criminal case 2551-10-12; criminal case 45296-11-12; various requests, criminal, 8177/20), and other cases involved flight expenses or the acquisition of equipment (computer, telephone, and so on) (serious criminal case 43935-05-10; criminal case 45296-11-12). Only one case involved provision of a more lucrative reward outside of a drug deal. This amount was estimated at 11,000 euros over six years of the agent's activity (serious criminal case 1625-08-08).

Table 6. Motivations for espionage

Motivation for spying	Number of agents
Monetary	24
Ideological	6
Psychological-mental	4
Unknown	4
Monetary/ideological	3

After the monetary motivation, the ideological motivation was most common, whether it was a principal or combined motivation. Two of the women carried out the acts of espionage based on a psychological-mental motivation as a main or combined motivation, and a third woman claimed that the motivation was psychological-mental out of a desire to appease others, but that judge had difficulty verifying the claim and therefore it was placed in the "unknown" category. There were also men who carried out the espionage out of a main or combined psychological motivation.

Table 7 offers several examples of quotations in the rulings that present the judge's decision and probation review regarding the motivation of the defendants. The examination of the motivations by the judge and the probation reviews shows that during the trial there was a serious desire of the State of Israel to understand the motivations that encouraged the Israeli residents to operate on behalf of Hezbollah.

Table 7. Quotations from the trials on motivation

Defendant	Motivation	Judicial decision / probation review regarding motivation
Omar al-Heib, an officer at the rank of lieutenant-colonel from Beit Zarzir. Active in 2002. Met with Hezbollah operatives at points on the border with Lebanon.	Monetary	*The charge*: Drug trafficking, supplying information to Hezbollah including revealing the movements of the commander of Northern Command, the deployment of tank positions, information on aircraft and observation and military positions near the border. *The judge's decision*: "This connection was over the telephone but also through the exchange of letters, which were attached to drugs or to money as the case may be… Given the character of the defendant, and in light of the fact that he carried out his actions mainly out of monetary greed, a real doubt remains on the question of whether it has indeed been proved to us that the defendant was aware, while carrying out his actions, that they could cause harm to the state's security" (m 3/02).
Dorit Edri (of Jewish descent), a resident of Kiryat Shmona. Romantic partner of Jamil Kahmouz, head of the spy ring. Active during the years 2001-2003. Not known if she met with Hezbollah operatives, but known that she met with other Israeli agents who operated on behalf of Hezbollah in Israel.	Monetary	*The charge*: Drug trafficking, acquiring binoculars and night vision equipment for Hezbollah, photographing military bases, photographing Kiryat Shmona, photographing the Gush Halav region and Mount Meron, the Margaliot lookout region, the Manara Cliff, and road numbers as they appear on the sides of road in the area of Margaliot and the north, shopping centers. *The judge's decision*: "The original indictment filed against Dorit attributed security offenses to her, as well as offenses according to the Dangerous Drugs Ordinance…As part of the plea bargain, all of the security sections were dropped, and they settled for her time in detention." The sections for aiding drug trafficking remained (criminal case 36/03).
Charlie Peretz (of Jewish descent), resident of Kiryat Shmona. Active during the years 2001-2003 as part of the Said ben Jamil Kahmouz spy ring. It is not known if he met with Hezbollah operatives, but it is known that he met with other agents who operated on behalf of Hezbollah in Israel.	Monetary	*The charge*: Drug trafficking, supplying information to Hezbollah, including publicly available literature with statistical data on Israel, and arms trafficking. *The judge's decision*: "According to the revised indictment, Peretz admitted that he trafficked only a dangerous hashish-type drug with a total weight of 80 kg." In the indictment, the security offenses regarding the transfer of information were dropped (criminal case 36/03).

Defendant	Motivation	Judicial decision / probation review regarding motivation
Isam Mishahara, resident of Jerusalem. Active in 2021. Met with Hezbollah operators in Lebanon.	Ideological	*The charge*: He did not manage to receive missions before he was caught, but while he was in Lebanon he identified on a map various sites in Jerusalem. *The judge's decision***:** "It is clear from the defendant's acts, from his consistent striving to make contact with Hezbollah personnel in Beirut, and from his willingness to meet with them and receive instructions, money, and means from them for carrying out activity after returning to Israel, that he displayed personal support for the Hezbollah organization and its aims, and this support is what was behind his actions" (criminal case 45296-11-12).
Manar Jabarin, resident of Umm al-Fahm. University student, active during the years 2003 to 2007. Met with a Hezbollah operator in Jordan.	Psychological-mental	*The charge*: Enlistment with Hezbollah and gathering information in Israel. *The judge's decision*: "The defense counsel retracted claims regarding their version of the mental state of the defendant at the time of carrying out the acts attributed to her and to the mental crisis that she was in at the time. We can learn from the defendant's representatives' claims that against the backdrop of the mental crisis claimed above and given that she was separated from her supportive environment, that is, her family, in a foreign country, she had difficulty coping with what they defined as 'conflictual emotional states,' which was exploited by the Hezbollah agent" (serious criminal case 4041/07).
Salim bin Said Abd el-Razek and Majd bin Adam Sirhan, both residents of Abu-Snan. Active in the year 2000. Met with Hezbollah operators at various points on the border with Lebanon.	Monetary/ ideological	*The charge*: Information on the deployment of IDF forces in the north and the movement of soldiers. *The judge's decision***:** "We have not ignored the fact that Defendant 1 operated out of purely nationalistic motives, while Defendant 2 also wanted to combine drug trafficking with his activity. In any case, the personal circumstances of the defendants are dwarfed by the severity of the offenses here" (criminal case 408/00).
Yasmin Jabr, resident of the Old City of Jerusalem, worked at the National Library. Active during the years 2015 to 2019. Met with operators in Lebanon and Turkey.	Unknown—hearings on the defendant continue to take place in various courts	*The charge*: Enlistment with Hezbollah, aid in recruiting agents. *The judge's decision*: "I did not find anything in the respondent's claims regarding the motivations that led her to perform the acts, and that certainly will become clear as necessary as part of the main proceedings, in order to lower the high level of danger posed by her, as previously stated" (various requests, criminal, 8177/20).

Charges and Extent of Damage

The list of charges reveals that first and foremost Hezbollah sought to gather military information on Israel (Table 8). This information was divided into two main areas—general information on the IDF, including the deployment of the IDF's forces, vehicles, locations of bases, and more, as well as specific information on the IDF in the north. In addition, Hezbollah's intelligence activity included a combination of drug and arms trafficking, i.e., intelligence information was supplied as part of drug and arms deals. Hezbollah also sought to identify civilian issues such as the mood in Israel and social and political issues, while likewise trying to base intelligence information on open source civilian information including books, civilian maps, and news articles.

Table 8. Charges

Charges	Number of charges
Supplying intelligence information on IDF forces in general, including information on sensitive military facilities in Israel, intelligence facilities, IDF invasion plans into Lebanon, bases of elite units, helipads in Israel, information on aircraft, and more.	27
Gathering precise information on the deployment of IDF forces in the north and the movement of soldiers. Gathering information on the village of Ghajar and vulnerabilities on the northern border, the names of bases and brigades, and the locations of observation posts and cameras on the border.	22
Trafficking of drugs (transporting/acting as a middleman between Hezbollah and distributors in Israel), weapons, and transferring general intelligence information about Israel.	17
Supplying open source civilian information, including information on civilian infrastructure, government ministries, shopping centers, and hospitals, as well as civilian documents—atlases, maps, books, news articles, and more.	10
Supplying information about people, including potential additional agents, collaborators with Israel in the village of Ghajar, and the activity of certain Israeli individuals.	3
Refusal to carry out missions: In three cases the defendants refused to carry out several actions that Hezbollah demanded. In one case the defendant refused to provide objects and equipment to other Hezbollah agents in Israel, but did cooperate on other intelligence issues (criminal case 4041/07). In a second case, one agent out of a network of three friends refused to perform security offenses (supplying information) out of an awareness of the potential security consequences, and focused only on transferring drugs, while the two other partners agreed to perform security offenses and drug offenses (various requests 001009/04). In a third case a female agent refused to continue to meet with her operator in Istanbul, Turkey, out of fear of being caught, after she had already met with him there once (various requests, criminal, 8177/20).	3
Operational activities, planning the placement of explosives at pick-up spots for soldiers, planning to carry out a terrorist attack within a military base.[1]	1

A basic question regards the extent and severity of the damage caused to Israel. According to the court, it is not possible to know what information the terrorist organization lacks that it seeks to acquire and how it will use the information that it obtains, and therefore it is sometimes difficult to determine the severity of the damage (various requests 04/001009). In the ruling on Manar Jabarin from Umm el-Fahm, a 24-year-old student who maintained an ongoing connection with Hezbollah for four years (2003-2007), the indictment claims: "There are many aspects of contact with a foreign agent. Sometimes what started as transferring an external memory card could end with passing on other information or equipment that who knows what damage it would cause" (various requests 07/4041).

The ruling (criminal case 45296-11-12) on Isam Mishahara, a resident of Jerusalem who operated on behalf of Hezbollah in 2012, described the way the defendant was asked to supply information on Israel before he managed to do so, but it is known that the defendant helped Hezbollah personnel locate important sites on a map. In the end, the court determined that this amounted to "potentially severe damage to the state's security," mainly because the defendant is a resident of Israel who can move freely in the country and gather sensitive military information (criminal case 45296-11-12).

In another ruling on the defendant Mahmoud Jabarin from Umm el-Fahm, a man born in 1983 who operated on behalf of Hezbollah in 2018, the court claimed: "Even if the defendant's actions did not cause overt and immediate damage, we cannot underestimate the severity of the defendant's actions and the importance of the cognitive war underway between Israel and its enemies. The defendant was aware of the use that Hezbollah makes of videos and knowingly continued to send them, out of identification with the organization's aims and knowing that this harms the state's security" (serious criminal case 51606-03-19).

Even when it comes to military information, there is not necessarily a consensus regarding the severity of the damage. For example, the indictment of Amar Khashima, born in 1978, married with two children, who worked as a school secretary and college teacher, notes that he supplied a large amount of military information to Hezbollah in 2009. This information included a description of the police's order of battle; a navy base in Eilat that also serves as a base for special units; an IDF base in Tel Aviv in which, according to him, the IDF reconnaissance Sayeret Matkal unit trains and where there is a helipad; information about various individuals, and more. The court claimed that some of the information was simple, and the information did not cause considerable damage (mainly because it was open source information), but according to the court it was still information that could cause potentially severe damage to the state's security (serious criminal case 09/652).

In certain cases, the court determined that supplying information to Hezbollah can cause significant damage, mainly if it is information that is difficult to obtain. The ruling on 26-year-old Milad Khatib from Majd al-Krum describes the complex military information that the defendant supplied to Hezbollah during the years 2007-2012, such as the precise locations where missiles fell in Israel, the locations of weapons and ammunition storage facilities in Israel, arms factories, and the security arrangements for the state's president. According to the prosecution, which was vindicated by the court, this amounted to "very significant damage, the provision of information to the enemy on places in which weapons are stored and produced, a place where important people are hosted, or the security arrangements of Israel's president, which could have been used by the enemy to cause heavy damage to the State of Israel" (serious criminal case 2551-10-12).

The ruling on Amir Mahoul, who operated in the service of Hezbollah for four years (2006-2010), noted that he even provided secret information to Hezbollah on ISA facilities in various cities in Israel, including the precise addresses of the buildings, their security arrangements, the locations of secret military bases, the locations of arms factories, and information on the strengths and weaknesses of Israeli society. The court saw these as severe offenses with "very real damage to the state's security," mainly because some of the information was secret (serious criminal case 43935-05-10).

A strict stance was also taken toward the defendant Omar al-Heib—an officer at the rank of lieutenant-colonel who operated in the service of Hezbollah for a full year. Al-Heib focused most of his activity for Hezbollah on smuggling drugs into Israel, but as part of this activity Hezbollah demanded that he supply military information about Israel. As a member of the military with an active position in northern Israel, al-Heib supplied secret information to Hezbollah, including information on the commander of the IDF's Northern Command, where he slept, the deployment of tanks in the northern region, command positions, and other secret information that was not revealed in the ruling. The court accepted the state's position that this amounted to significant military harm, especially because of the sensitive information that the defendant supplied to Hezbollah.

The damage caused by supplying information to Hezbollah was mainly potentially severe damage to Israel's security. The information supplied to Hezbollah was diverse and the organization based its intelligence picture of

Israel on it. Some of the information was secret military and security information, while other information was available open source and in part also civilian information. There is no doubt that presenting secret information to Hezbollah could cause military damage to Israel, but it appears that most of the damage caused was potential military damage, depending on how Hezbollah used the information or could use the information in the next campaign.

Tools

The operation of the agents and the transmission of information usually occurred through technological means, including cell phones, encrypted communication programs available on the internet, various communication applications, social networks, and more (Table 9). This method of transmission enabled the operator and the agent to maintain distance from one another and still to transmit information between them. Other information was transmitted through documents, verbally, and in face-to-face meetings. These meetings were usually more dangerous, but in many cases they were the result of additional activity such as drug and arms trafficking, which in any case required that the two sides transmit information and physical equipment between them. Some of the agents employed several espionage tools simultaneously.

Table 9. Means for communication and for transmission of information

Espionage tools	Frequency
Mobile phone	17
Transmitting information verbally / face to face	12
Internet—encrypted programs, communication applications, email	6
Social networks on the internet	5
Documents: books, maps, pictures, and journalism	5
Other: memory devices or unknown means	5

Conclusions

Terrorist organizations are non-state actors that operate intelligence units for the purpose of gathering intelligence on their adversaries out of an intent to learn about them, identify weaknesses and strengths, plan terrorist attacks, and advance counterintelligence purposes. The use of intelligence by terrorist organizations is diverse and includes technological intelligence and human intelligence (Bitton, 2019; Gentry, 2016; Shapir, 2017). The intelligence gathering methods of a terrorist organization are not substantially different from the methods used by a sovereign state. While there may be a significant gap in their respective resources, terrorist organizations have certainly begun to develop intelligence units and methods that are very similar to the intelligence methods of a sovereign state (Tsichritzis, 2015).

In analyzing the modes of operation of 41 espionage agents in Israel by Hezbollah, no clear personal profile of the agents was found. While most were Arab men, their age range was broad, and their education and family status were diverse. Regarding the modus operandi of agents, however, several frequent patterns can be identified. A large portion of the agents chose at their own initiative to operate on behalf of Hezbollah; most of the agents chose to operate out of a monetary motivation, and the next most prominent motivation was ideological. Most of the agents were caught within a short amount of time from when they were recruited—possibly due to low-level espionage skills and poor training (along with Israeli intelligence superiority). Most of the agents supplied military information about Israel, and the communication between the agents and their operators was based primarily on phone communication and direct meetings.

In many cases, enlistment with Hezbollah occurred at the initiative of the agents, especially after they had sought to engage in drug trafficking or to operate out of ideological opinions. Other cases of recruitment occurred at Hezbollah's initiative, usually as part of meetings abroad. Until 2006, Hezbollah succeeded in operating spy rings that included several agents, but after 2006 the number of spy rings declined and their sized was reduced, and Hezbollah began to operate individual agents. It is certainly possible that the changes that occurred after the Second Lebanon War, due to the UN's decision prohibiting the presence of a military force in southern Lebanon (except for the Lebanese army) (IDF website, 2018), made it difficult for Hezbollah to operate along the border fence and to recruit large spy rings, and therefore the organization began to engage in recruiting individual agents. In addition, Hezbollah never abandoned its attempts to recruit and operate agents in Israel, even when agents that it operated were exposed again and again. In the end, Hezbollah succeeded in recruiting agents in Israel, whether in large networks or as individuals. The dozens of agents that Hezbollah operated in Israel allowed the organization to be exposed to military information, secret information, and open source civilian information about Israel.

The intelligence information that was supplied to Hezbollah mainly had the potential for future harm to Israel's security. That is, even though the agents were exposed within a short time, they managed to supply military and civilian information to Hezbollah. The severity of the damage cannot yet be determined unequivocally; it remains to be seen how Hezbollah acts in a future armed conflict with Israel. The study showed that the information gathering process is analogous to continuously putting together a puzzle that includes open source intelligence, human intelligence, and technological intelligence, and enables reaching insights on the adversary's military capabilities, its strengths and weaknesses, and its civilian society in general. Whether the information is gathered from open source literature and journalism or whether it is secret information, it enables putting together an intelligence picture of the adversary and exploiting this in the future.

When Hezbollah recruited the agents, it identified and exploited their psychological-emotional weaknesses, the economic troubles of several residents of Israel, and the ideological hatred harbored by several agents, and based on these characteristics, the organization succeeded in operating agents on its behalf. Monetary, ideological, and psychological motivations were considered the most common motivations for operating agents in Israel, and thanks to Hezbollah's human intelligence system, which is deployed in various countries in the world, it has succeeded in identifying these main motivations and operating agents in Israel from a distance.

Most of the agents acted out of a monetary motivation, either as a principal motivation or in combination with a secondary motivation. The monetary motivation was identified mainly in men; some acted out of financial distress and others out of a desire to increase their income.

But despite the recruitment of dozens of agents who operated on behalf of Hezbollah in Israel, many were exposed within a short time. The study showed that Israel's intelligence superiority and the fact that on several occasions Hezbollah has rushed to operate agents in Israel without rigorous preparation for them led to the quick exposure of the agents in Israel. Hezbollah's intelligence capabilities are considered moderate compared to Israel's counterintelligence capabilities, especially because of the gaps in resources and skills between the adversaries (Harber, 2009; Tsichritzis, 2015).

The modus operandi of operating Hezbollah agents in Israel showed that in many cases they were new, inexperienced operatives who had not yet proven their potential in the organization. At the same time, it was noted in the literature survey that Hezbollah's agents are identified with various professional skills; some of them are people with military training or training from the organization (abroad), and others were characterized by a lack of training, espionage inexperience, and a lack of understanding regarding the activity that they carried out, which led to their quick exposure. This could also explain why most of the intelligence agents that were operated in Israel did not fulfill simultaneous operational roles that sometimes require unique additional skills such as constructing explosive charges and operating weapons, because some of the agents did not at all see themselves in combat roles and operational activities. A few agents engaged in drug trafficking and saw their main activity as smuggling drugs and weapons and not necessarily espionage, while others were recruited by chance (as part of a trip abroad) and were immediately demanded to operate on behalf of Hezbollah.

The operation of agents is a complex and prolonged process, but it appears that sometimes Hezbollah rushed to operate agents and did not train and operate them professionally and properly. The recruitment and operation of agents on a poor professional level alongside Israel's intelligence superiority enabled Israel to expose most of the agents within a relatively short time. Yet even though Israel succeeded in exposing Hezbollah agents repeatedly, the organization did not despair at the quick exposures and continued to engage constantly in recruiting intelligence agents in Israel. This emphasizes the extent to which Hezbollah sees supreme importance in recruiting agents in Israel, and it attempts to do so again and again.

Gil Riza has a degree in industrial engineering and management from Ruppin College (2002-2004), a Bachelor's degree in political science and international relations from the Open University (2005-2008), and a Master's degree in Counter-Terrorism Studies from Monash University in Australia (2010-2012). He completed an internship at the Department of Premier and Cabinet in Victoria, Australia, in the Security and Emergency (2012). Today he is an independent researcher on terrorism. gilriza@yahoo.com

References

Bitton, R. (2019). Getting the right picture for the wrong reasons: Intelligence analysis by Hezbollah and Hamas. *Intelligence and National Security*, *34*(7), 1027-1044. https://doi.org/10.1080/02684527.2019.1668717

Buhbut, A. (2015, August 14). The ISA's battle of brains against Hezbollah's spy unit. *Walla!* https://news.walla.co.il/item/2881262 [in Hebrew].

Buhbut, A. (2016, January 21). Failure after failure: This is how Hezbollah has been trying to insert agents into Israel for 20 years. *Walla!* https://news.walla.co.il/item/2927362 [in Hebrew].

Gentry, J. A. (2016). Toward a theory of non-state actors' intelligence. *Intelligence and National Security*, *31*(4), 465-489. https://doi.org/10.1080/02684527.2015.1062320

Harber, J. R. (2009). Unconventional spies: The counterintelligence threat from non-state actors. *International Journal of Intelligence and CounterIntelligence*, *22*(2), 221-236. https://doi.org/10.1080/08850600802698200

Hezbollah activity with Israeli Arabs. (2014, September 13). Israel Security Agency. https://bit.ly/36mSQlF [in Hebrew].

IDF reveals additional position of terrorist organization Hezbollah. (2018, October 22). IDF. https://bit.ly/3un4yEY [in Hebrew].

Kulick, A. (2009). Hizbollah espionage against Israel. *Strategic Assessment*, *12*(3), 119-132. https://bit.ly/3p1ONBa

Levitt, M. (2020). Breaking Hezbollah's "golden rule": An inside look at the modus operandi of Hezbollah's Islamic Jihad organization. *Perspectives on Terrorism*, *14*(4), 21-42. https://www.jstor.org/stable/26927662

Lillbacka, R. (2017). The social context as a predictor of ideological motives for espionage. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 117-146. https://doi.org/10.1080/08850607.2016.1230704

Lt. Col. H., Major Bar Gil, & Major (res.) T. (2021, October 3). Hacking for influence: Resilience as a tool for coping with Iran's cyberwarfare. Dado Center. https://bit.ly/3tvYpqz [in Hebrew].

Michael, K., & Dostri, O. (2018). The Hamas military buildup. In A. Kurz, U. Dekel, & B. Berti (Eds.), *The crisis of the Gaza Strip: A way out* (pp. 49-60). Institute for National Security Studies. https://bit.ly/3aizijQ

Penal Law 1977. Nevo. https://bit.ly/3twQ0TS [in Hebrew].

Pop, I., & Silber, M. D. (2021). Iran and Hezbollah's pre-operational modus operandi in the West. *Studies in Conflict & Terrorism*, *44*(2), 156-179. https://doi.org/10.1080/1057610X.2020.1759487

Riedel, B. (2011). Terrorist intelligence capabilities: Lessons from the battlefield. *Georgetown Journal of International Affairs*, *12*(1), 26-33. https://www.jstor.org/stable/43133861

Shapir, Y. S. (2017). Hezbollah as an army. *Strategic Assessment*, *19*(4), 67-77. https://bit.ly/3iwRYNY

Siboni, G., Cohen, D., & Rotbart, A. (2013). The threat of terrorist organizations in cyberspace. *Military and Strategic Affairs*, *5*(3), 3-29. https://bit.ly/3HvT9cd

Siboni, G., & Kronenfeld, S. (2015). Developments in Iranian cyber warfare 2013-2014. In G. Siboni (Ed.), *Cyberspace and national security: Selected articles III* (pp. 61-82). Institute for National Security Studies. https://bit.ly/3xICQ7p

State Comptroller (2021). *National preparedness for defending against the threat of drones: Expanded follow-up*. Annual report 71b. https://bit.ly/3IrMkqQ [in Hebrew].

Strachan-Morris, D. (2019). Developing theory on the use of intelligence by non-state actors: Five case studies on insurgent intelligence. *Intelligence and National Security*, *34*(7), 980-984. https://doi.org/10.1080/02684527.2019.1672034

Thompson, T. J. (2014). Toward an updated understanding of espionage motivation. *International Journal of Intelligence and CounterIntelligence*, *27*(1), 58-72. https://doi.org/10.1080/08850607.2014.842805

Tsichritzis, G. (2015). *Intelligence collection, analysis and reporting of terrorist groups: A study on effectiveness*. Research Institute for European and American Studies. https://bit.ly/3D2KgEG

Wege, C. A. (2016). Anticipatory intelligence and the post-Syrian war Hezbollah intelligence apparatus. *International Journal of Intelligence and CounterIntelligence*, *29*(2), 236-259. https://doi.org/10.1080/08850607.2016.1121039

Zeitoun, Y., Rubinstein, R., Morag, G., & Curiel, I. (2021, December 16). Dressing up as a delivery person and photographing the Iron Dome: Resident of Jaffa and Gaza trader charged with spying for Hamas. *Ynet*. https://bit.ly/3mGZlEo [in Hebrew].

Appendix: List of rulings by start date of agent's activity (some rulings include several defendants)

[District] Criminal case 408/00 State of Israel vs. Salim bin Said Abd el-Razek (Haifa), June 13, 2001

[Supreme] Various requests, criminal, 224/04 State of Israel vs. Jamal bin Naaf Rahal, January 13, 2004

[District] Criminal case 36/03 State of Israel vs. Said bin Jamil Kahmouz (Nazareth), July 15, 2007

[Military] M 3/02 Military prosecutor vs. Omar al-Heib, April 27, 2006

[District] Serious criminal case 1625-08-08, State of Israel vs. Khaled Kashkush (center), January 7, 2009

[District] Various requests 001009/04State of Israel vs. Mahmad bin Abdo Shmali (Nazareth), January 14, 2004

[District] Serious criminal case 4041/07 State of Israel vs. Manar Jabarin (Haifa) November 28, 2007

[District] Various requests 1234/06 State of Israel vs. Jamil bin Salah Abu Salah (Haifa) March 26, 2006

[District] Criminal case 536/06 State of Israel vs. R.B.M.M. (Nazareth), May 21, 2007

[Magistrate] Various requests 1837/07 Attorney General vs. Azmi Bishara (Petach Tikva), April 25, 2007

[District] Serious criminal case 43935-05-10 State of Israel vs. Amir Mahoul (Haifa), January 30, 2011

[Supreme] Various requests, criminal, 4664/13 Zahr Yusufin vs. State of Israel, July 8, 2013

[District] Serious criminal case 2551-10-12 State of Israel vs. Milad Khatib (Haifa), April 9, 2013

[Supreme] Various requests, criminal, 120/10 State of Israel, Rawi Sultani, February 24, 2010

[District] Serious criminal case 652/09 State of Israel, Jerusalem District Attorney vs. Amar Khashima (Jerusalem), March 22, 2010

[District] Remand 10-07-1390 State of Israel vs. Osama Waked (Nazareth), October 7, 2010

[Military] Appeal (district) 73/11 Wahib Salman vs. Military Advocate General, November 25, 2012

[District] Criminal case 45296-11-12 State of Israel vs. Isam Mishahara (Jerusalem), October 21, 2013

[Supreme] Various requests, criminal, 8177/20 State of Israel vs. Yasmin Jabr, November 26, 2020

[District] Serious criminal case 51606-03-19 State of Israel vs. Mahmoud Jabarin (Haifa), March 8, 2021

[District] Serious criminal case 52144-03-20 State of Israel vs. Mai-Bat Masarawa (center), December 1, 2021

Notes

[1] On several occasions Hezbollah attempted to use agents in Israel for operational objectives such as terrorist attacks, placement of explosives, kidnapping, arms smuggling, and more. Because these activities did not always include the supply of intelligence, they were not included in the case studies in this study. Additional cases of Hezbollah agents in Israel for operational activities appear on the ISA website (ISA, 2017. See also https://www.shabak.gov.il/publications/Pages/shotef080812.aspx [in Hebrew].