Mitzpe Institute
בהירות למי שפועל

Forensic intelligence for those who act.

READER EDITION | November 27, 2025

MITZPE DOSSIER

The Digital Battlefield

◇ URIEL ZEHAVI

CLASSIFICATION Reader Edition
DISTRIBUTION Open · Free to share with attribution

IN THIS EDITION

Field Dossier: The Digital Battlefield 3

Jews, Israelis, and Zionists on the grid while others hunt for their footprints. 3

The Digital Battlefield: How Jews, Israelis, and Zionists Get Targeted One Click at a Time 3

The Adversaries: Who Is Hunting 4

How They Work: From Footprint To Target 6

Digital mobbing and doxxing 7

Hack-and-leak intimidation 7

Honey traps and social engineering 7

Harassment as theater 8

Mass panic messaging 8

What It Looks Like From The Couch 8

Different Theaters, Same War 10

Hardening Against Exposure 11

What They Want From Your Screen 12

Field Dossier: The Digital Battlefield

JEWS, ISRAELIS, AND ZIONISTS ON THE GRID WHILE OTHERS HUNT FOR THEIR FOOTPRINTS.

By Uriel Zehavi · [illegible] November 27, 2025

We spend a lot of time here talking about rockets, militias, Iran's money pipelines, and the ridge over Ben Gurion. That is still the main story. It probably always will be. Though, I'd love, one day, to just send a single line: "All is ok, read something else." Not sure that's a likely outcome.

That said, there is another front where the same enemies reach for you without crossing a border, without smuggling a rifle, without sending a single "activist" down your street. They don't need to. You already walked into range with your phone, your inbox, your child's school newsletter, your synagogue's website.

That front is the digital battlefield.

You do not have to be a public figure to be on it. You only have to exist as a Jew, an Israeli, or a visible supporter of the Jewish state in an age where everything about you leaks through a screen.

So let's pull the camera back.

This Dossier maps how hostile states, terror groups, extremists, and bored cowards on message boards turn ordinary digital life into a hunting ground. We will walk through what they want, how they look for it, the shortcuts they take, and what you can do to make their job harder.

Think of this as a field brief for people who assume they are "too small" to matter. You are not.

If Hamas can reach a conscript in an army base through a fake Instagram account, if an Iranian front can dump the medical records of strangers in Tel Aviv, if a doxxing mob in Boston can publish a spreadsheet of Jewish preschool teachers, then the distance between "online" and "my front door" is already gone.

The goal here is simple: clarity, then action.

What is this battlefield. Who fights on it. Where normal people are exposed. And how you harden your life without turning into a hermit.

The Digital Battlefield: How Jews, Israelis, and Zionists Get Targeted One Click at a Time

In Judea and Samaria, the fight often begins with arguments over names. "West Bank" turns a three-thousand-year Jewish history into a generic edge of a river. The label itself shifts everything. Online, something similar happens, but with your life.

We talk about "content," "activity," "engagement," as if the internet were just entertainment. Underneath the marketing fluff sits a harsher truth: every

post, every like, every sign-up form is a piece of terrain. Someone can stand on it, shoot from it, or build a road across it.

Your Instagram feed that shows which café you visit on Fridays. Your LinkedIn that lists your employer or your campus. Your synagogue's bulletin posts your name on the "Welcome New Members" page is there for all to see. Your high school alumni list that mentions you attended a Jewish day school. Your mother's Facebook post brags about your IDF service.

None of that feels dangerous. It feels normal. That is the problem.

Modern digital life produces three kinds of ground.

First, the open street. Public profiles, tweets under your real name, event flyers, news articles that quote you. Anyone can see them without logging in. This is where most attackers start. A search box and some patience are enough.

Second, the back alleys. Semi-private group chats, mailing lists, password-free "members' areas," cloud documents that were meant to be internal but sit one careless click away from public. You might think you are in a tucked-away hallway. Chances are that you're not.

Third, the hidden rooms. The data you never see but others store. Databases at companies, schools, charities, airlines. Data brokers who buy and sell lists of names, phones, and addresses. Government files. Once those are breached or sold, strangers know more about you than your neighbors.

States, terror groups, and freelance haters operate across all three. They walk the street, peer into alleys, and break into rooms. You experience the result as a single hit: a flood of threats, a hacked account, your name on a map.

If you imagine the internet as neutral territory where "everyone is just posting," you will never build the right defenses. This is not neutral. It is contested ground.

The Adversaries: Who Is Hunting

The actors on this front are not random. Some wear uniforms and medals, some banners and ski masks, some hoodies and anonymity. Their motives differ; their interest in you does not.

First, state regimes that see the Jewish state and Jewish communities as fair game.

Iran sits at the top of that list. Tehran's security services run hackers, proxies, and fake "activist" brands that stretch from the Gulf to European capitals. They do classic intelligence work—spear-phishing diplomats, trying to get into defense networks—but they also aim lower. They go after journalists, academics, small-time Israeli businesspeople abroad, anyone whose kidnapping or humiliation would pay a political dividend.

In several cases, Iranian operatives posed as scholars and NGO staff, using LinkedIn and email to invite Israelis and Jews to "conferences" in friendly

cities. The real itinerary ended with a kidnapping squad waiting at the airport. Those plots were foiled, but the method tells you everything. The regime looked at professional networking as a hunting tool, not a business utility.

Groups with names like Black Shadow and Moses Staff, widely linked to Iran, breached Israeli companies, then dumped stolen data not for ransom, but for pain. Medical records, LGBTQ dating profiles, ID card scans. The victims were not generals. They were ordinary citizens told by a hostile power: we hold your secrets, and we can humiliate you on demand.

Second, terror organizations that have learned to fish in the digital pond. Hamas is not a meme factory. It is an armed Islamist movement that happens to be very comfortable on Android.

For years, its cyber unit has run a simple, effective play against Israeli soldiers: build fake personas of attractive women, send friend requests, start flirtatious chats, join WhatsApp groups, and eventually offer some app to "share photos" or "boost phone performance." Once installed, that app turns the phone into a sensor. Camera, microphone, GPS, contacts, stored photos—the whole lot. The IDF has publicly described rounds of these operations, each time finding new spyware in soldiers' phones.

The stakes are obvious. A single infected phone in a combat unit is a live feed into tent life, vehicles, and briefing rooms. It reveals patterns: when a base is busy or quiet, when a platoon rotates, which road they use home. That is targeting data.

Hamas and Palestinian Islamic Jihad also use basic social engineering elsewhere. Fake NGOs contacting activists. "Journalists" seeking comments. Telegram channels run by handlers disguised as supporters, trying to pull in Israelis and diaspora Jews.

Third, extremist networks on the far-right, the far-left, and the jihadist fringe.

White supremacists in the United States have been using the internet to target Jews since dial-up. The template is familiar. A neo-Nazi site picks a target—say, a Jewish woman who had a dispute with a prominent racist—and posts her phone, email, and family information with a call for a "troll storm." Hundreds of men then hammer her with calls, voicemails, emails, and messages about ovens, gas, and bullets. They trawl through her social feeds for photos of her children, then mention those kids by name in threats.

A digital mob aimed at breaking a person psychologically. The ease with which it happens rests on the amount of information the target left available.

On the far-left and within some "anti-colonial" circles, the language changes, not the method. Activists build so-called "mapping projects" that present Jewish charities, schools, and even arts organizations as nodes in a sinister Zionist network. Each node includes names, addresses, and staff roles. The call to arms is wrapped in academic jargon, but the message is simple: these people live here, go deal with them.

Islamist extremists add a religious gloss. For them, a Jewish journalist in London or a synagogue president in Paris is not just a political opponent;

he or she is an enemy of God. That matters when you decide how seriously to take their threats.

Fourth, hacktivists and freelance doxxers. They might not answer to a state or cell. They do answer to the dopamine hit they get from "exposing" someone. Students who compile "Zionist watchlists" on campus. Anonymous accounts that trawl LinkedIn for employees of Israeli companies and post their faces under slogans about genocide. Self-appointed vigilantes in Boston who decide that every Jewish preschool is fair game for an interactive "map of oppression."

These operators often use openly available tools: OSINT search engines, facial recognition services, public registries. The barrier to entry is low. Ten minutes on Google and a petty grudge can turn into a full doxx.

The lines blur. A doxxing list produced by anonymous activists might later be scraped by an Iranian intelligence unit, then shared with a Hamas-run Telegram channel, then land on a neo-Nazi forum. Once your details are out, you do not control who uses them or why.

How They Work: From Footprint To Target

Digital targeting rarely feels like a spy movie. It feels boring, then shocking.

Most attack chains begin the same way: someone looks for an easy mark. That means an exposed footprint and a clear payoff.

A Jewish student posts under her full name about Israel on a public account. A synagogue publishes a PDF membership directory with names and emails. A small Jewish nonprofit leaves its website admin panel with a default password. A soldier accepts a friend request from a stranger with a pretty profile picture. A LinkedIn profile shows "IDF reserves, intel background" in the bio.

From there, the attacker meanders a simple path.

First step: collection. They search your name, screenshot your posts, right-click your photos, dig through followers and friends. They try people-search sites. They check if your email appears in any data breaches. They note your job, school, or shul.

Second step: connection. They contact you or move closer. A DM, an email, a fake job invite, a "journalist" query. Or they skip talking to you and approach your employer, your university, your landlord, your neighbors, armed with "evidence" curated from your online life.

Third step: action. That could be doxxing—posting your info with a call to harass. It could be a phishing email designed around your habits. It could be malware delivered through a convincing pretext. It could be sending messages to your friends trying to scam them out of money. It could be an attack on your bank account. It could be a kidnapping plan using your travel schedule.

A few concrete patterns show up again and again. You're never too small to be at risk.

DIGITAL MOBBING AND DOXXING

When Hamas attacked on October 7th, the information war lit up in parallel. In North America and Europe, Jewish students and professionals who took even mild pro-Israel positions found their inboxes flooded. Anonymous posters built "Zionist lists" with names and photos harvested from campus club pages and LinkedIn. Those lists often included contact details. One man in Philadelphia who spoke about Hamas online ended up with his email and address blasted out; harassers then called him fifty times an hour and sent death threats. That is what turning a digital footprint into a weapon looks like.

In Australia, activists infiltrated a WhatsApp group for Jewish creatives and academics. They leaked the entire chat history and member list online. Hundreds of Jews who thought they were talking among friends suddenly saw their names, emails, and in some cases addresses exposed to a hostile world. Some were threatened. Some were vandalized. One group of strangers captured the private life of six hundred people because someone clicked "join chat."

HACK-AND-LEAK INTIMIDATION

The Black Shadow breach in Israel, backed by Iran, followed a related pattern at a higher level. Hackers broke into a web host, pulled massive amounts of customer data from a gay dating app, a travel insurer, and a clinic, then dumped the data publicly, taunting victims.

They didn't want to scam them for money—not much at least. No. They wanted to make people anxious and afraid. Gay Israelis were outed to families and employers. People saw their ID scans and medical files posted on Telegram channels run by clerics in Tehran who consider them fair game. The message from the regime was blunt: we can reach into your private life with a keystroke.

HONEY TRAPS AND SOCIAL ENGINEERING

The Hamas honey-trap operations against IDF soldiers are a masterclass in low-tech human hacking. Some of the apps they used were custom, but the rest were almost insultingly simple. Fake women's accounts, flattery, patience, and a promise of more intimate content if the soldier installs an app, clicks a link, or just sends another selfie from their unit.

Hostile actors exploit ordinary desires and loneliness. Once the phone is infected or the WhatsApp group compromised, the soldier's unit becomes a set of dots on a map. The operator on the other end can watch, listen, and take notes. Which base has poor discipline. Which patrol route repeats. Which corner of a staging area holds sensitive gear. How to disable or operate a tank.

Iran's lures to pro-Zionist activists and former Israeli officials abroad follow the same logic. You get a polished email from a think tank offering a paid speech in Istanbul or Dubai. The invite references your real work. The logo is real. The "organizer" has a LinkedIn profile with dozens of connections.

Very few people would suspect that behind the keyboard sits an intelligence officer whose goal is to hand your room number to a hit team.

HARASSMENT AS THEATER

In the United States, a neo-Nazi site owner handed out a Jewish woman's personal information and told his followers to "send a message." They did. Gunshot sounds on the phone. Promises that her child would be thrown in a gas chamber. Hundreds of messages over weeks. No one needed advanced skills. They needed a target, a phone number, and encouragement.

On campuses, the same pattern plays out with more progressive branding. Anonymous posters distribute flyers naming Jewish students as "supporters of genocide." Online, those names get tied to petitions, boycott calls, and coordinated shaming. Many of the participants tell themselves they are engaging in "accountability." In practice, they are participating in the same kind of swarm the neo-Nazis run, just with different slogans.

MASS PANIC MESSAGING

During the current war, Israelis have received spoofed SMS messages claiming their loved one has been captured, or that their bank is about to freeze accounts unless they click a link. Some of these campaigns trace back to Hamas or allied hackers, who used bulk texting tools and caller-ID spoofing to mimic Israeli numbers.

The aim is to sow chaos and distrust. If you cannot trust the message from an official app or a familiar number, every siren and every buzz becomes suspect. That erodes resilience long before the first line of code does technical damage.

The theme through all of this: attackers do not need to break a bank's vault. They can walk through the unlocked side door of your digital house. The easier you are to map, the easier you are to reach.

What It Looks Like From The Couch

It is one thing to talk about tactics. It lands differently when you imagine it as part of your own life.

Picture a college student in the United States. She runs her campus Hillel's Instagram. The account posts Shabbat dinners and joint events with Black and Hispanic student groups. After October 7th, she posts a simple Israeli flag with a short message about grief.

Within a day, the comments fill with abuse. Some accounts are real classmates. Others are anonymous or foreign bots. A Tumblr blog springs up listing "Zionists on campus," and her photo—scraped from her personal account—sits near the top. Her university email appears next to it. Soon she gets threats: some juvenile, some detailed. A fake journalist writes asking for comment "before we publish what we know about you." She has an exam the next morning.

Or think about a suburban family in New Jersey. The local paper runs a story on a solidarity rally after a synagogue is vandalized, and quotes the father,

David, as a volunteer leader. His name hits Google. A white supremacist forum picks up the article and posts his name and city under a thread about "Jew enemies in small towns." An eager user spends ten minutes on a people-finder site and posts David's full address and a Google Street View shot of his house.

Within days, David's voicemail fills with accusations and threats. Someone starts ordering pizzas and deliveries to his home as a "joke." His teenage kids find their TikTok accounts spammed with comments linking back to the thread. When David walks his dog at night, he wonders whether the car slowing near his driveway is just lost or something else.

Or take a Jewish teacher in Paris. He is not an activist. He teaches French, coaches a little basketball, and shows up at shul. His name appears on an alumni page for a Jewish high school and on a sports club Facebook album.

Activists building a "Zionist network" list scrape those pages and add him. He spots his own name for the first time when someone sends him a link: an infographic naming him a collaborator in "apartheid," with his school labeled as a node in a web of evil. A few weeks later he notices unfamiliar faces lingering outside his building after work, staring at him, then looking at their phones. One morning the wall near his apartment door has fresh graffiti with his surname and a slur.

Or look at a former IDF soldier back at university in Tel Aviv. Her mother in the United States posts a proud Facebook announcement with photos of her in uniform and the unit number on her shoulder patch. That post is public.

An anti-Israel hacker group scrapes posts containing unit names. They match her face to her own private Instagram, which has looser approvals than she remembers. They pull her Israeli phone number from an old leak. They send a fake WhatsApp from "a former comrade," with an attachment of "funny photos from base." She taps it between classes. The malware now lives on her phone.

Weeks later, she sees her own name and photo in a Telegram channel where Iranian and Palestinian users gloat about "tracking Zionist pigs." They include her home neighborhood and mention that her brother currently serves in an active unit. She has never posted about him once.

Or maybe you're an outspoken supporter of Israel volunteering for a nonprofit. Your friend posts that you two are going on a trip with a stopover in Istanbul or Paris. Or perhaps a conference in Texas near a Sharia stronghold. Iran decides to activate a local cell to humiliate the West and to ransom you. You did buy kidnap insurance, right?

None of these people is a general, a minister, or a billionaire donor. They are targets because they are visible at just the right size: easy to reach, not important enough to have a security detail.

The digital battlefield shrinks the distance between a troll, a foreign intelligence officer, and your living room. That is the point. It is cheaper than rockets and easier to deniably outsource.

Different Theaters, Same War

The way this plays out changes with geography.

In the United States, Jews live in a country with strong speech protections and very weak privacy protections. You can say almost anything about anyone online and often get away with it. At the same time, your address, phone, and email are for sale to anyone with a credit card.

American Jews, especially on campus, face mobs from both ends of the spectrum. Neo-Nazis organize "troll storms." Far-left coalitions run doxxing campaigns and social boycotts. The ADL recorded historic highs in antisemitic incidents since October 7, much of it tied to Israel rhetoric and amplified online.

So a Jewish student at Columbia or Berkeley navigates a public square where you can be hounded day and night, and where the infrastructure of harassment sits one Google search away. The upside is that law enforcement and civil courts have space to move once threats cross into criminal territory. The downside is the time and courage required to march through that process when you are twenty and just trying to pass exams.

In Europe, Jews live closer to the physical edge. European states have more aggressive hate-speech statutes and data protection rules. That can make open online abuse riskier for perpetrators. So some of the worst activity moves into encrypted channels and closed groups: Telegram networks, far-right forums hosted abroad, jihadist chat rooms. It festers there and then spills over into the real world.

Antisemitic assaults and vandalism have long been part of life in Paris, London, Berlin, Brussels. A large share of Jews there report hiding Jewish symbols in public, including online, to avoid trouble.

Iran and its friends have focused on Europe as a playground. They plot against synagogues in Germany, Israeli embassies in London, Jewish and Israeli targets in Istanbul or Cyprus. These plots start with online surveillance: watching who posts where, who travels, who works in what embassy. The gap between online recon and a physical attack is smaller when hostile intelligence services operate in your postal code.

In Israel, as always, the cyber and kinetic fronts blend.

The same actors who gun down families on roads invest in phishing and ransomware. Civilian data is a target not for profit, but for pressure. When Black Shadow dumped the information of Israeli LGBTQ users and patients, it was a message: we can pry into your private life whenever Tehran wants.

At the same time, Israelis are heavy users of social media and group messaging. WhatsApp groups for every class, unit, and community. Facebook pages for every cause. That makes coordination easier during emergencies; it also gives attackers countless avenues for infiltration.

Israelis have an advantage: many go through the army, where basic security discipline gets drilled in. Suspicious links. Device rules. Awareness of enemy

cyber activity. That training fades over time for some, and family members who never served often lack it. Of course, it doesn't always work when you're partially raised by TikTok. That said, a twenty-year-old conscript may reject a suspicious DM; his father might click the same link.

Regardless of location, however, the enemy correctly bets that Jews and Israelis will treat the internet as a source of entertainment long after it became a live front.

Hardening Against Exposure

You cannot control Iran. You cannot re-educate a Hamas hacker or a bored neo-Nazi. You can control your own attack surface.

Digital hygiene is not paranoia. It is a set of habits that make it harder and more expensive to target you. For state-level enemies, it forces them to waste time and money on higher-value targets. For lone doxxers and campus mobs, it denies them the easy thrill they crave.

Think about it the way the IDF thinks about ground.

You cannot stop every rocket, but you can put early-warning systems, interceptors, and shelters in place. You cannot guarantee no terrorist ever enters one area or another, but you can control critical junctions, lookouts, and depth of protection.

On the digital front, the same logic applies. You build three kinds of defenses.

First, personal posture. That is what you control alone. Privacy settings. Passwords. Your instinct to click or not click. How much you share on public feeds. Whether you think about your kids' exposure when relatives post their faces.

If you have not done this yet, do a simple exercise. Open a private browser window. Search your own name. Add your city. Add your school. Add "email." Whatever you find there is what an attacker finds in the first two minutes. Do you see your home address? Job? Children's names? Synagogue? Old comments you forgot. That is your baseline picture.

Think about how easily someone can put together where you are likely to be and when. What pressure points they can hit. A call or text, purporting to be your rabbi, referencing your kids or a shared event, and then what? Financial scam? Harassment? Assault? All very easy pickings, unfortunately.

Second, family and community posture. You are only as protected as your most careless relative.

Parents who tag their teenager's high school in every sports photo. Grandparents who post the full itinerary of a grandchildren's trip to Israel. Synagogue staff who upload PDFs of membership rosters without a password. Campus groups that publish officer lists with emails and dorms.

Talk to them. Not in panic tones. In the same way you would talk about locking the front door or not giving your social security number to a telemarketer.

Set house rules. No posting children's school names publicly. No tagging soldiers in uniform—you don't even need unit numbers, facial recognition allows them to be targeted everytime they have a trip abroad. No posting live locations from rallies. Ask your shul and school what they publish and how they protect lists. If they do not have answers, push.

Third, structural resilience. That is the ability to take a hit and keep functioning.

Assume, for a moment, that you have been doxxed. Your name and address are out in the wild. Strangers send vile messages. Someone spams your boss with accusations. The first instinct is to retreat.

A better instinct is to move through a script.

Document everything. Screenshots. Email headers. Links. File that with police, campus security, or communal security bodies. Most Western countries treat threats and harassment as crimes—when you can convince them to do so you'll find that evidence matters.

Reach out to your network. Let your rabbi, dean, employer know what is happening before they get a call from a troll pretending to be an angry citizen. Most institutions prefer to stand by the person who came to them early.

Change what you can. New phone number if needed. Stronger passwords. Locked-down profiles. Consider freezing your credit if identity theft seems likely.

Above all, refuse to let hostile actors dictate your presence. Sometimes you will choose to step back from visible roles to protect your family. That is legitimate. Just make sure it is a choice, not a reflex born from shock.

For those with higher profiles—journalists, rabbis, visible activists, donors—the defensive posture needs more rigor. Hardware keys for logins. Separate devices for sensitive work. Encrypted email. Professional incident response contacts.

This may shock you, but unfortunately it shouldn't any longer. But many of the habits dissidents in Iran, Russia, and China use belong in the toolkit of outspoken Jews in the West now. Enemy regimes already see you on the same map. Sadly, you're used to seeing visible security in Jewish spaces... this is the natural extension of that.

What They Want From Your Screen

Every conflict comes down to intent.

In Judea and Samaria, the ridge is not about housing. It is about whether a hostile army can point artillery at Israel's core.

In the digital theater, the same clarity applies.

Iran's goal is not entertainment. It wants leverage over citizens of the West and of Israeli society. It wants dissidents, LGBTQ Israelis, public servants, and ordinary citizens to live with a sense of vulnerability. A hacked file here,

a leaked database there, a humiliation campaign now and then. The aim is to erode trust in the state's ability to protect its people and to strip away the feeling that your private life is your own.

Hamas and its fellow militias want intelligence, fear, and recruitment. Intelligence for targeting soldiers and bases. Fear to sap Israeli morale and Jewish diaspora activism. Recruitment of sympathizers radicalized online through propaganda and mobbing.

Far-right and far-left extremists want something simpler: a world where Jews shut up and disappear from public life. They do not need to physically attack every Jew. It is enough if enough Jews decide that speaking as Jews carries too much cost.

When "Mapping Projects" pin Jewish preschools and charities to hate maps, when campus lists label Jewish students as enemies, when neo-Nazis and "anti-colonial" activists talk about "disrupting networks," they are engaged in the same project: criminalizing visible Jewish life.

The point of doxxing a Jewish creative in Sydney or a teacher in Paris is not to win an argument about Gaza. It is to send a signal to everyone watching: this is what happens when a Jew steps forward. Stay in your lane, keep your head down, and maybe we will leave you alone.

Strip away the slogans on both ends, and you are left with a familiar demand: Jews can exist quietly in private, if at all, but not proudly. Not as a nation. Not in public. And certainly not as armed sovereigns on their own land—its anathema to centuries of pervasive rot.

The digital battlefield is one more route to that same goal.

The answer cannot be passivity. Nor can it be hysteria and retreat from every platform. We do not abandon Judea and Samaria because they are targeted. We harden them. We do not close Ben Gurion because someone wants to hit it. No, we build layers of defense around it.

The same goes for the digitized elements of your life.

Harden your accounts, your habits, your family's instincts. Shrink the easy attack surfaces. Accept that enemies are watching. Refuse to live as if that means your voice, presence, or Jewish identity must vanish.

There is one Jewish state. There is one dispersed Jewish people. Both now stand not only on physical soil but on digital ground. That ground is contested.

You cannot negotiate with people who treat your existence as the problem. You can frustrate them. You can deny them easy wins. You can build a culture where Jews and Israelis know that the phone in their hand and the laptop on their desk sit on the same front as the ridge over Ben Gurion.

ABOUT THE AUTHOR

Uriel Zehavi

EXECUTIVE DIRECTOR · MITZPE INSTITUTE

Uriel Zehavi is the executive director of Mitzpe Institute, where he writes the daily Israel Brief and co-directs its Institutional Intelligence practice with Modi Zehavi. He is the author of four books from Mitzpe Press and advises Israeli and allied clients on strategic communications for Western audiences.

ABOUT MITZPE INSTITUTE

Mitzpe Institute is an intelligence and strategy organization focused on Israeli security, diaspora threat assessment, and the strategic challenges confronting the Jewish people and the West. We produce daily intelligence, forensic analyses, strategic assessments, and tactical briefings read by policymakers, military leaders, and institutional decision-makers across more than 90 countries and all 50 US states — from the Knesset and the US Congress to allied governments, major policy institutions, and Jewish organizational leadership worldwide.

PASSED ALONG TO YOU?

The daily Israel Brief is free at mitzpe.org. The operational layer — Closed Dossiers, Vantage, and Watchwords — is members-only. Become a member, gift a membership, or book a briefing at mitzpe.org.