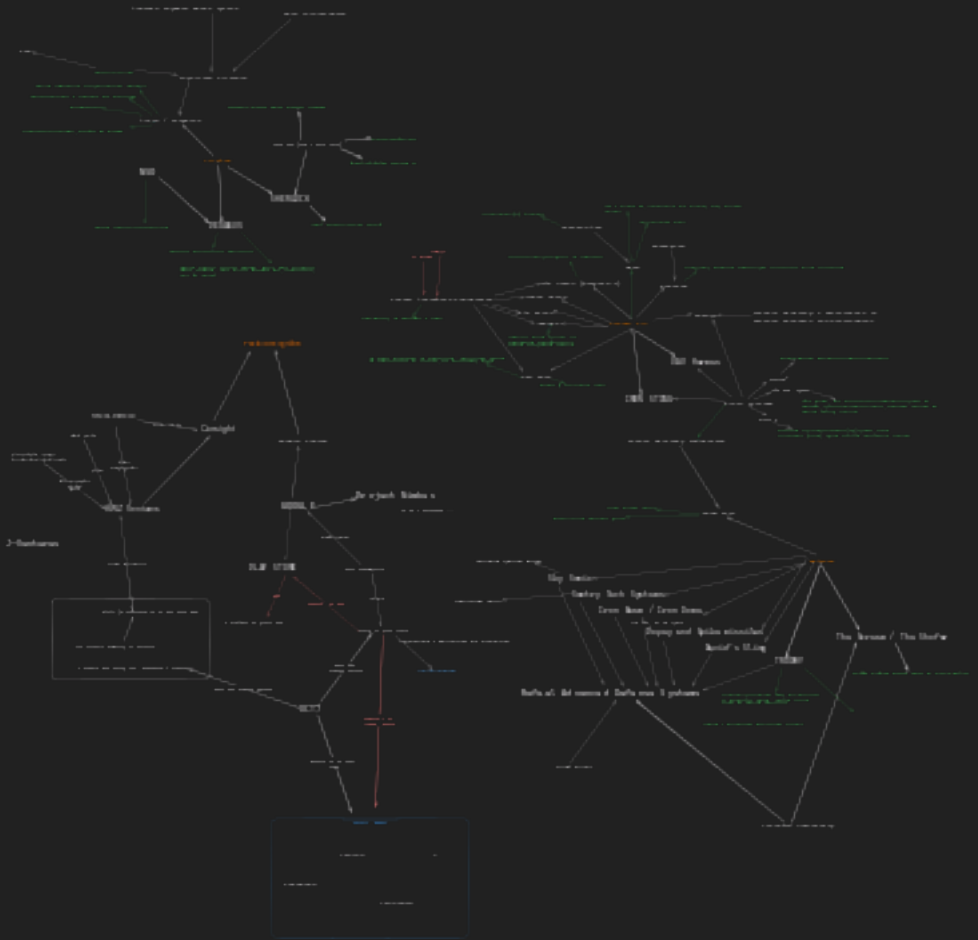


# Genocidal Tech Map



2024-10-01

# Contents

- \* Social Media, Influence & Censorship
  - \* J-Ventures Global Kibbutz Group
  - \* Project "Iron Truth"
  - \* OCT7
  - \* Social Fighters
  - \* Project "Digital Dome"
  - \* Google Maps / Apple Maps / Bing Maps / Mapquest / Yandex Maps
  - \* GoFundMe / Paypal / Venmo
- \* Infrastructure and Compute
  - \* Project Nimbus
  - \* Dream AI
- \* Military targeting
  - \* Habsora בשורה ("The Gospel")
  - \* Lavender (+ Where's Daddy?)
- \* Weapons
  - \* The Scream / The Shofar
  - \* TROPHY / missile systems like David's Sling, Popey and Spike / missile defense systems like Iron Beam and Iron Dome / Sentry Tech System
  - \* Iron Fist (Hebrew: חץ דורבן)
- \* Drones
  - \* Elbit Systems
  - \* Israel Aerospace Industries
  - \* Rooster
  - \* ROBUST, the acronym for ROBOTic aUtonomous Sense and strike
  - \* HERO loitering systems
  - \* Aeronautics
- \* Research & Development
  - \* Universities
- \* Surveillance
  - \* Mabat 2000 / SMART M / SAIP / OSCAR
  - \* Mispar Hazak
  - \* Palantir Technologies
  - \* Basel System / Maoz System
  - \* PIBA (Israeli Population, Immigration and Border Authority)
  - \* Aviv system
  - \* Meitar system
  - \* Al Munasq
- \* Spyware
  - \* Pegasus

- \* [Sherlock / custom Candiru spyware](#)
- \* [Alien / Predator](#)
- \* [Incarceration](#)
  - \* [G4S security systems / G1 Secure Solutions](#)
  - \* [IPS Kabarnit Plan](#)
- \* [Intelligence](#)
  - \* [Unit 8200](#)
- \* [Image, Text, and Facial Recognition](#)
  - \* [Homeland Security Text Mining](#)
  - \* [Corsight](#)
  - \* [COGITO4M / COGITO 1003 / SmartForms AI](#)
  - \* ["Better Tomorrow" / Google Avosh / OnWatch / OnAccess / OnPatrol / SesaMe](#)
  - \* [Blue Wolf](#)
- \* [Venture Capital](#)
  - \* [AWZ Ventures](#)
  - \* [Selling software to ISF](#)
- \* [How to contribute](#)
- \* [Reading list \(to do\)](#)

## Social Media, Influence & Censorship

The removing of pro-Palestinian & anti-Israelian content through various means such as (automatically) flagging social media posts for removal. It also entails the organising and coordinating of pro-Israeli comments on anti-Israeli posts as well as shadowbanning, the censoring of accounts or actively reducing the reach of pro-Palestine content.

[TODO: explore this source and complete entry] Source: <https://www.aljazeera.com/features/2023/10/24/shadowbanning-are-social-media-giants-censoring-pro-palestine-voices>

Firm: Facebook, Instagram, X, YouTube and TikTok  
Technical Mean: hide #hashtags with ...  
Objectives: Target: Effects:

## **J-Ventures Global Kibbutz Group**

A collaboration between pro-Israeli investors, tech executives, activists, and government officials. They collaborate to fire anyone arguing in favor of Palestinian freedom, including Courtney from Wix, and Paddy Carey Cosgrave from Websummit, and to put public pressure on any comments deemed anti-Israel.

### Firm

J-Ventures, a U.S.-Israeli investment fund. Oded Hermoni, the project's WhatsApp group's founder, is a managing director of J-Ventures.

### Technical Means

A WhatsApp group which serves as a kind of coordination centre where a group of independent players in Silicon Valley's pro-Israel community exchange ideas, identify enemies, and collaborate on ways to defend Israel in the media, academia, and the business world. The group includes prominent Silicon Valley venture capitalist Jeff Epstein – a former CFO of Oracle – and Andy David, a diplomat-cum-venture capitalist who also serves as the Israeli foreign ministry's head of innovation, entrepreneurship, and tech.

### Sources

\* [Inside the Pro-Israel Information War](#) All-Source Intelligence Fusion (08-12-2023).

## Project “Iron Truth”

A group of volunteers from Israel's tech sector removing anti-Israeli content from social media platforms.

### Firm

n.a. Initiator - Dani Kaganovitch, a Tel Aviv-based software engineer at Google. The effort is run by volunteers and is not officially initiated or led by any corporation. Partners with OCT7, an Israeli group that “monitors the social web in real-time ... and guides digital warriors,” and Israeli Ministry for Diaspora Affairs. Promoted by Israeli American investment fund J-Ventures.

### Technical Means

Flagging content manually and through OCT7's API and app.

### Objectives

Removal and censorship of anti-Israeli content on social media, including blocking efforts to fundraise for Gaza.

### Target

LinkedIn, Facebook, TikTok, YouTube, Google app store and more.

### Effects

The removal of roughly 1,000 posts tagged by its members as false, antisemitic, or “pro-terrorist” across platforms such as X, YouTube, and TikTok. Public face is a Telegram bot that crowdsources reports of “inflammatory” posts, which Iron Truth's organizers then forward to sympathetic insiders. 7amleh has documented over 800 reports of undue social media censorship since the war's start. Removal of NoThanks, an Android app that helps users boycott companies related to Israel, from Google app store.

### Sources

\* [Israeli Group Claims It's Working With Big Tech Insiders to Censor “Inflammatory” Wartime Content](#) The Intercept (10-01-2024)

## OCT7

“Unifying the Counter-Hate Warriors”. OCT7 “monitors the social web in real-time, identifying both positive and negative posts, and guides digital warriors—both individuals and organized groups—to engage effectively.”<sup>[1]</sup>

Collaborates with: Project Iron Truth, Words of Iron, Israeli American Council, Ministry of Diaspora Affairs, ZWST (Central Welfare Board of Jews in Germany), Social Fighters (fighthamas.co.il).

### Technical Means

An API through which you can flag social media posts as ‘good’ or ‘bad’ after which OCT7 will “make sure good things happen to it”. The API allows contributions through tagging as well as pulling data. OCT7 also offers an app through which users can process social media posts <sup>[1]</sup>.

### Objectives

Censorship of anti-Israeli social media content.

### Sources

\* <sup>[1]</sup> [oct7](#)

\* <sup>[2]</sup> [Israeli Group Claims It's Working With Big Tech Insiders to Censor "Inflammatory" W  
artime Content](#) The Intercept (10-01-2024)

## Social Fighters

Allied with OCT7.

Technical means

A website on which you can click and thereby post pre-written pro-Israeli replies to pro-Palestinian or anti-Israeli content on social media such as X/Twitter and YouTube. It's private Facebook group has 5.500 followers.

Sources

\* [Fight Hamas!](#)



## Project “Digital Dome”

volunteer effort led by the Israeli anti-disinformation organization FakeReporter. #####  
Firm Israeli anti-disinformation organization FakeReporter + volunteers. Promoted by  
Israeli American investment fund . ##### Objectives helps coordinate the mass  
reporting of unwanted social media content Target: ... Effects: ... ##### Source -  
<https://theintercept.com/2024/01/10/israel-disinformation-social-media-iron-truth/> -  
Facebook Censors Discussion of Rights Issues - [https://www.hrw.org/  
news/2021/10/08/israel/palestine-facebook-censors-discussion-rights-issues](https://www.hrw.org/news/2021/10/08/israel/palestine-facebook-censors-discussion-rights-issues)

## Google Maps / Apple Maps / Bing Maps / Mapquest / Yandex Maps

An Israeli official told Al-Arabiya, “We try to ensure that we are not photographed at high resolutions, and most (countries) accommodate us.” [4]

Firm

Apple said it was working to update its maps soon to a higher resolution. Google: its images come from a range of providers and it considers “opportunities to refresh [its] satellite imagery as higher-resolution imagery becomes available”. But it added that it had “no plans to share at this time”.v[2]

Technical Mean

At the height of the violence, open source investigators on Twitter noted that regions such as Gaza appear much blurrier on platforms like Google Earth, which collects satellite imagery from a variety of sources. The reason is an obscure US regulation, called the Kyl-Bingaman Amendment, that used to forbid American companies from providing higher-resolution satellite images of the region due to security concerns expressed by Israel. The regulation was scrapped last year, and the limit is now similar to the resolution allowed for other parts of the world. Many commercial satellite imagery providers, such as Planet Labs, quickly adjusted their products, while popular free tools, including Google Earth, did not. [6] “When searching for “Palestine” on Google Maps, the map zooms in on the Israel-Palestine region, and both the Gaza Strip and West Bank territories are labeled and separated by dotted lines. But there is no label for Palestine. In an email statement, Google said it doesn’t label the borders because there isn’t international consensus on where the Palestinian borders are located. Other major mapping companies approach this decision in different ways. When doing a general search for “Palestine,” here’s what happens:

Apple Maps, similar to Google, zooms in on the region but doesn't label it.

Bing Maps identifies a point on the map and labels it as "Palestine."

MapQuest identifies a point on the map and labels it as 'State of Palestine.'

Yandex Maps outlines Palestine's borders and labels it as 'Palestine.'

Objectives

Marwa Fatafta, a policy analyst at the Palestinian policy network al-Shabaka, said the decision was not surprising, considering that Google is “lending its cloud service to the Israeli government & their military apparatus”. [5]

## Target

Eyal Weizman, the founder of Forensic Architecture, a research agency that does similar open source investigations in the Middle East, agrees that the degraded images harm his work. “It reduces the capacity to monitor Israeli violations,” he says, and it puts the Israeli state in a position of power over Palestinians. “Israel controls what Palestinians can see.” [6]

## Effects

The International Committee of the Red Cross has operated in Israel and Palestine since the 1960s, offering health services and other assistance to people during and after outbreaks of violence. It also helps communities rebuild. The ICRC is making repairs to the water system, the power network, and the sewage system in the Gaza Strip. Many of those activities involve the use of satellite images. “During times of conflict, we use imagery to detect the extent of damages and destruction,” says Christoph Hanger, a spokesperson for the ICRC. And when it’s allowed to enter a conflict zone, it uses imagery to plan its movements. [6] Digital mapmaking in Palestine and Israel therefore can be seen as both a response to the need to administer contested lands and an enabling mechanism that allowed for maps to be made at much greater resolution at ever-finer scales. [3] international landscapes shape knowledge about Palestine and Israel as well as for a more in-depth account of the role that landscapes play in the production of international technoscience [3] Open-source investigators, however, rely heavily on the free-to-use mapping software and don’t often have direct access to these high-resolution images.[2]

## Sources

[1] <https://eu.usatoday.com/story/news/factcheck/2021/05/21/fact-check-google-maps-does-not-label-palestine/5145256001/> [2] <https://www.bbc.com/news/57102499> [3] Mapping Israel, Mapping Palestine - Jess Bier (2017) [4] <https://www.motherjones.com/politics/2011/06/google-israel-us/> [5] <https://www.middleeasteye.net/news/israel-gaza-google-no-plans-update-blurry-maps> [6] <https://www.wired.com/story/blurry-satellite-images-palestine-israel-make-rebuilding-harder/>

## GoFundMe / Paypal / Venmo

there's a complex web of red tape and corporate interests that undergird the supposedly seamless digital transfers that happen online every day. PayPal, for example, has refused to allow Palestinians to use its service for years, even as Israelis in illegal West Bank settlements are able to. In 2021, when violence broke out between Israel and Hamas, Venmo (which is owned by PayPal) was found to be delaying payments that included terms like "Palestinian emergency relief fund" and "emergency Palestinian relief fund." [1] In a cryptic, automated email, El-Sabawi was told that her PayPal account was being frozen due to "customers [being] dissatisfied with activity from this business". [4]

### Technical Mean

But what fundraiser organizers see as heavy-handed moderation has slowed down aid efforts, and inconsistent policies have left organizers and donors confused. Multiple organizers for fundraisers related to Palestine have received the same form email from GoFundMe referring to "the crisis unfolding in the Middle East," requiring them to provide additional information and documentation. These additional hurdles are baffling to the organizers, many of whom have run GoFundMe campaigns for other causes and have never encountered this extra red tape. [3]

### Target

Palestinian companies and organizations have repeatedly asked PayPal to make its service available to Palestinians in Gaza and the West Bank, but the company has so far declined. A report published in 2018 by the Arab Center for the Advancement of Social Media, a non-profit advocacy organization, found that "this inequality in access to financial services," makes it difficult for many Palestinians to participate in the global market. [2]

### Effects

Martin, who studies tech policy, says that humanitarian organizations have historically wrestled with the tension between verifying that funds or other types of aid are not reaching sanctioned groups or individuals. The task is "practically impossible," Martin says. [3] there is a growing amount of evidence to suggest that Western financial institutions are disproportionately freezing transactions to Palestine [4] humanitarian aid to Gaza is facing blockades of every kind from Western institutions and far-right Israeli groups. Meanwhile, Palestinians are killed, wounded, and starved in their tens of

thousands.[4]

## Sources

[1] <https://www.business-humanrights.org/en/latest-news/palestine-organizers-nonprofits-criticize-gofundmes-handling-of-urgent-life-saving-gaza-donations/>

[2] <https://restofworld.org/2021/venmo-palestinian-relief/>

[3] <https://www.theverge.com/2024/2/29/24085175/gofundme-gaza-palestine-fundraiser-under-review-esims>

[4] [How pro-Israel saboteurs are derailing lifesaving Gaza fundraisers](#) - The New Arab, 17th April 2024

## STOIC

Fake social media accounts used for Israeli propaganda found by Digital Forensic Research Lab, and de-activated by Meta

Firm

STOIC a political marketing and business intelligence firm based in Tel Aviv, Israel

Technical means

“This network’s accounts posed as locals in the countries they targeted, including as Jewish students, African Americans and ‘concerned’ citizens. They posted primarily in English about the Israel-Hamas war, including calls for the release of hostages; praise for Israel’s military actions; criticism of campus antisemitism, the United Nations Relief and Works Agency (UNRWA), and Muslims claiming that ‘radical Islam’ poses a threat to liberal values in Canada” [META Adversarial Threat Report]

- \* 510 Facebook accounts, 11 Page, one Group
- \* 32 Instagram accounts [META Adversarial Threat Report]
- \* 130 suspicious X accounts [Digital Forensics Research Lab]

Objectives

- \* Astroturf support for Israel
- \* de-legitimise US campus protests
- \* Amplify criticism of UNWRA

Sources

[Meta report reveals anti-UNRWA campaign linked to Israel-based intel firm](#) The New Arab, 30 May 2024

[META Adversarial Threat Report - First Quarter](#) May 2024

[Suspicious accounts on X amplify allegations against UNRWA](#) Digital Forensic Research Lab, 14 Feb 2024

## Infrastructure and Compute

## Project Nimbus

A \$1.2 billion cloud computing system jointly built by Google and Amazon, Israel's "official cloud".

### Firms

IDF, Google and Amazon

### Technical Means

Google cloud platform's machine-learning and AI tools, with capacity for facial detection, automated image categorization, object tracking, and even (scientifically unproven) sentiment analysis that claims to assess the emotional content of pictures, speech, and writing. "Faces, facial landmarks, emotions"-detection capabilities of Google's Cloud Vision API, an image analysis toolset. Edge applications allow for remote and autonomous ('cloudless') application of these services through for instance phones or bodycams.

### Objectives

Undisclosed. Surveillance, analysis and control.

### Effects

"Google's machine learning capabilities along with the Israeli state's surveillance infrastructure poses a real threat to the human rights of Palestinians," according to Amnesty International's Algorithmic Accountability Lab's Damini Satija. Google is contractually obliged to abide by Israeli law and isn't allowed to shut down or retract its services and claims it cannot oversee what clients do with its products. According to Jack Poulson, director of the watchdog group Tech Inquiry, another effect is that Project Nimbus is "preventing the German government from requesting data relating on the Israel Defence Forces for the International Criminal Court".

### Sources

\* [Documents Reveal Advanced AI Tools Google Is Selling to Israel](#) The Intercept (24-07-2022)

\* [No Tech for Apartheid](#)



## Dream AI

The name of the company - Dream - derives from an abbreviation of Detect, Respond and Management

### Firm

Dream security: a “pioneering AI cybersecurity company delivering revolutionary defense through artificial intelligence” [2] - From its inception, Dream Security’s strategy was based around an in-house connection to the international right.[1] - Founders are in the board of HaShomer HaChadash, active in illegal outposts in the West Bank [1] - Dream is staffed in part by NSO veterans. [1]

### Technical Mean

- \* “Dream’s advanced AI automates discovery, calculates risks, performs real-time threat detection, and plans an automated response. With a core focus on the”unknowns,” our AI transforms data into clear threat narratives and actionable defense strategies. ... At the core of our solution is Dream’s proprietary Cyber Language Model, a groundbreaking innovation that provides real-time, contextualized intelligence for comprehensive, actionable insights into any cyber-related query or threat scenario” [2]

### Objectives

- \* “Our proprietary AI platform creates a unified security system safeguarding assets against existing and emerging generative cyber threats.” [2]
- \* “Revolutionizing Digital Reality: Leveraging AI to counter AI threats, pioneering national-level Cybersecurity” [3]

### Target

- \* organizations with industrial installations in energy, water and health infrastructures.

### Sources

- \* [1] <https://theintercept.com/2024/01/18/israel-nso-group-shalev-hulio-dream-security/>
- \* [2] <https://www.linkedin.com/company/dreamsecurity/>
- \* [3] <https://www.dreamgroup.com/>

## Military targeting

## Habsora בשורה (“The Gospel”)

An “AI” that automatically produces targets for shelling, first used during Israel’s 11-day war with Hamas in May 2021 [3].

### Firm

The Targets Administrative Division of the Military Intelligence Directorate of the IDF. It has put together a database containing 30.000-40.000 suspected militants, and was started in 2019 [4].

### Technical Means

Habsora, an AI tool rapidly generating targets for shelling, trained on data gathered by the IDF’s intelligence branch. Supposedly an algorithm is used which determines in real-time how many civilians remain in a residence, there is no empirical evidence indicating this is functional or accurate (whole residential areas are flattened).

### Objectives

The official objective is the real-time automatic generation/suggestion of targets allowing the army to carry out strikes (shelling) on residential homes where suspected Hamas members live (including junior members), on a massive scale. The unofficial objective is identifying ‘power targets’ (“matarot otzem”), killing large amounts of civilians, to “create a shock” among civilians that, among other things, will “lead civilians to put pressure on Hamas,” [1]. “there is a growing sense that the country is now using AI technology to excuse the killing of a large number of noncombatants while in pursuit of even low-ranking Hamas operatives.” [2]

### Target

Residential homes (called ‘power targets’) During the first five days of fighting, half of the targets bombed – 1,329 out of a total 2,687 – were deemed power targets.

### Effects

Habsora can generate >100 targets per day of which 50% is attacked (including homes of suspected junior Hamas members), the number of civilians who may be killed in attacks on private residences is known in advance to Israeli intelligence, and appears clearly in the target file under the category of “collateral damage.” The IDF works with

a 'collateral damage directive' number, for instance if the number is 5, any residence with 5 or less civilians can be attacked. Every attack is approved by IDF operators.

## Sources

- \* [1] ['A mass assassination factory': Inside Israel's calculated bombing of Gaza](#) +972 Magazine (30-11-2023).
- \* [2] [Israel's Military-Technology Complex Is One of a Kind](#) Foreign Policy (19-12-2023).
- \* [3] ['The Gospel': how Israel uses AI to select bombing targets in Gaza](#) The Guardian (01-12-2023).
- \* [4] [IDF intel unveils new Targeting Center](#) Israel National News (14-03-2019).

## Lavender (+ Where's Daddy?)

A system to mark suspected operatives in the military wings of Hamas and Palestinian Islamic Jihad (PIJ), including low-ranking ones, as potential bombing targets. The “Where’s Daddy?” system tracked these targets and signaled to the army when they entered their family homes.

### Firm

- \* All these technologies are developed by Israeli companies, which sell them to the Israeli armed forces and then export them to other countries, claiming that they have been tested in the field. [4]

### Technical Means

- \* The Lavender software analyzes information collected on most of the 2.3 million residents of the Gaza Strip through a system of mass surveillance, then assesses and ranks the likelihood that each particular person is active in the military wing of Hamas or PIJ. According to sources, the machine gives almost every single person in Gaza a rating from 1 to 100, expressing how likely it is that they are a militant. [1]
- \* everyone in Gaza has a private house with which they could be associated, the army’s surveillance systems could easily and automatically “link” individuals to family houses. In order to identify the moment operatives enter their houses in real time, various additional automatic softwares have been developed. These programs track thousands of individuals simultaneously, identify when they are at home, and send an automatic alert to the targeting officer, who then marks the house for bombing. One of several of these tracking softwares ... is called “Where’s Daddy?” [1]
- \* “How do we do it? We take original subgroups, calculate their close circle [of personal connections], calculate relevant features, rank results and determine thresholds, use intelligence officers’ feedback to improve the algorithm,” and then use classified digital platforms to locate the targets. [5]

### Objectives

- \* Lavender marks people – and puts them on a “kill list”. (NB. fundamental difference with the Gospel that marks buildings and structures)[1]
- \* An IDF statement described Lavender as a database used “to cross-reference intelligence sources, in order to produce up-to-date layers of information on the military operatives of terrorist organisations. This is not a list of confirmed military operatives eligible to attack.[6]
- \* intelligence personnel “manually” checked the accuracy of a random sample of several

hundred targets selected by the AI system [1]

## Target

- \* marking tens of thousands of Palestinians using AI [1]
- \* under “Operation Iron Swords,” the army decided to designate all operatives of Hamas’ military wing as human targets, regardless of their rank or military importance. [1]
- \* even some minors were marked by Lavender as targets for bombing [1]

## Effects

- \* during the first weeks of the war, the army almost completely relied on Lavender, which clocked as many as 37,000 Palestinians as suspected militants – and their homes – for possible air strikes [1]
- \* the system makes what are regarded as “errors” in approximately 10 percent of cases, and is known to occasionally mark individuals who have merely a loose connection to militant groups, or no connection at all (including police and civil defense workers, militants’ relatives, residents who happened to have a name and nickname identical to that of an operative, and Gazans who used a device that once belonged to a Hamas operative) [1]
- \* when it came to targeting alleged junior militants marked by Lavender, the army preferred to only use unguided missiles, commonly known as “dumb” bombs (in contrast to “smart” precision bombs), which can destroy entire buildings on top of their occupants and cause significant casualties. [1]
- \* according to two of the sources, the army also decided during the first weeks of the war that, for every junior Hamas operative that Lavender marked, it was permissible to kill up to 15 or 20 civilians [1]
- \* Lavender and systems like Where’s Daddy? were thus combined with deadly effect, killing entire families, sources said. By adding a name from the Lavender-generated lists to the Where’s Daddy? home tracking system, A. explained, the marked person would be placed under ongoing surveillance, and could be attacked as soon as they set foot in their home, collapsing the house on everyone inside. [1]

## Sources

- \* [1] ‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza](<https://www.972mag.com/lavender-ai-israeli-army-gaza/>), +972 Magazine, April 3, 2024
- \* [2] [Meta and Lavender](#) Paul Biggar (to check?)
- \* [3] [Why human agency is still central to Israel’s AI-powered warfare](#) +972 magazine, April 25 2024
- \* [4] <https://english.elpais.com/technology/2024-04-17/lavender-israels-artificial->

intelligence-system-that-decides-who-to-bomb-in-gaza.html

\* [5] <https://www.jpost.com/israel-news/article-731443>

\* [6] <https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-amas-airstrikes>

## Weapons



## The Scream / The Shofar

The 'Scream' is a 'non-lethal' acoustic system that 'creates sound levels that are unbearable to humans at distances up to 100 meters', according to Technion. It has been nick-named 'the Shofar', a horn blown on High Holy Days as a reminder to repent for the sins of the past year; apparently the Palestinians must repent for Israel's war crimes.

Firm

Technion University

Target

The police responded to the protests with means to disperse them, including water cannons, horses, and, unusually, even a "Tzeaka" ('scream' in Hebrew) system that emitted disturbing sound waves toward the protesters. In response to a Walla query due to the unusual use of the system - which can lead to pain and even be a health hazard - The police admitted that the use of the system was used by accident. [2]

Effects

This crowd-control weapon is mainly used to suppress peaceful demonstrations in the occupied Palestinian territories (Lee, 2017).

Sources

[1] <https://www.eccpalestine.org/beyond-dual-use-israeli-universities-role-in-the-military-security-industrial-complex/> [2] <https://www.jpost.com/israel-news/article-794875>

## **TROPHY / missile systems like David's Sling, Popey and Spike / missile defense systems like Iron Beam and Iron Dome / Sentry Tech System / Sky Sonic**

TROPHY Active Protection System (APS) ... can be integrated with all vehicle classes – tanks or APCs, wheeled, tracked, MBTs, and 8x8s – and is the only fully-integrated APS fielded by NATO. Fully tested, qualified, and extensively combat-proven in hot zones around the world, TROPHY integrations include the US Army's Abrams MBTs, Israel's Merkava MBTs and Namer APCs, the UK's Challenger MBTs, and Germany's Leopard 2 MBTs.

### Firm

Rafael Advanced Defense Systems Ltd. "It was founded as Israel's National R&D Defense Laboratory for the development of weapons and military technology within the Israeli Ministry of Defense" [2] From 2011 to 2021, the United States contributed a total of US\$1.6 billion to the Iron Dome defense system,[11] with another US\$1 billion approved by the US Congress in 2022. [4] "True to its origins at the facilities of the Weizman institute and the Technion, Rafael still calls itself 'the national laboratory of Israel'. Rafael was not the only weapons company birthed by Israeli academia." [10]

### Technical Mean

" Creating a neutralization bubble around a vehicle, TROPHY engages all known threats – including recoilless rifles, ATGMs, AT rockets, HEAT tank rounds, RPGs and low-signature threats – ensuring crew and vehicle survivability and maneuverability. the system successfully neutralizes enemy anti-tank teams in fractions of seconds, locating the fire source and enabling return fire" [1] MPrest agreed to sell 50 percent of its equity to state-owned Rafael Ltd., prime contractor for Iron Dome: MPrest Systems Ltd., developers of the Iron Dome's battle management control (BMC) system, an embedded mission simulator allows soldiers to train on the same equipment that will soon be entrusted with defending against enemy salvos launched beyond Israel's borders. Known here as Iron Glow, the BMC system automatically integrates, classifies and filters data from numerous airborne and ground-based sensors, serving up a cohesive, comprehensible picture of the tactical environment. [7]

### Objectives

"Saving lives since 2011, TROPHY transforms any combat platform into an ultra-modern, highly lethal, and survivable machine – enabling exceptional maneuverability

for forces in the field. Assured of their safety, ground units are free to rapidly advance and strike, allowing mission completion and uninterrupted combat continuity.” [1] - the Israeli Border Control Sentry-Tech turret currently deployed along Gaza’s border. They were designed to prevent Palestinians from leaving the Gaza strip and entering Israeli territory. Automated ‘Robo-Snipers’ set up along the Gaza border, designed to create “automated kill-zones” at least 1.5 km deep. But they aren’t merely robotic guns. The turrets feature heavy duty 7.62 calibre machine guns tied into a network spanning the entire border. If any turret detects human movement, the entire chain of guns can train their sights and concentrate firepower on the interloper. Some turrets are also able to fire explosive rockets. [8] -it is developing the Sky Sonic, an air defence system that will be capable of intercepting hypersonic missiles [11]

## Target

In October 2023, the Ministry of Defense and Rafael announced that they would deploy Iron Beam to the southern border with the Gaza Strip to test it with rocket barrages fired by Hamas during 2023 Israel–Hamas war. [3]

## Effects

Rafael, whose products include the Iron Dome air defense system and the Trophy active protection system used on Israel’s main battle tanks and APCs, plays a central role in the current war effort. [6] More than 40,000 missiles from the Spike family have already been supplied to countries around the world and over 7,000 of them have been fired, both as part of training routines and in operational use on the battlefield. [5] Omar Shakir, the Israel and Palestine Director at Human Rights Watch, said Israel is on a “slide toward the digital dehumanization of weapons systems.” By using such technologies, Shakir said Israel is creating “a powder keg for human rights abuse.” [9]

## Sources

[1] <https://www.rafael.co.il/system/trophy-aps/> [2] [https://en.wikipedia.org/wiki/Rafael\\_Advanced\\_Defense\\_Systems](https://en.wikipedia.org/wiki/Rafael_Advanced_Defense_Systems) [3] [https://en.wikipedia.org/wiki/Iron\\_Beam](https://en.wikipedia.org/wiki/Iron_Beam) [4] [https://en.wikipedia.org/wiki/Iron\\_Dome](https://en.wikipedia.org/wiki/Iron_Dome) [5] <https://en.globes.co.il/en/article-rafael-wins-naval-maintenance-and-anti-tank-missile-deals-1001454890> [6] <https://breakingdefense.com/2024/03/rafael-expects-iron-beam-laser-to-be-active-in-2025-exec/> [7] <https://web.archive.org/web/20110720134604/http://www.tsjonline.com/story.php?F=4265663> [8] <https://www.trtworld.com/magazine/israel-s-autonomous-robo-snipers-and-suicide-drones-raise-ethical-dilemma-44557>

[9] <https://apnews.com/article/technology-business-israel-robotics-west-bank-cfc889a120cbf59356f5044eb43d5b88> [10] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) p92 [11] <https://defence-industry.eu/rafael-ready-to-collaborate-with-european-industry-on-hypersonic-technologies/>

## Iron Fist (Hebrew: חץ דורבן)

a hard-kill active protection system (APS) designed by Israel Military Industries (IMI), with a modular design allowing adaptation to a range of platforms ranging from light utility vehicles to heavy armoured fighting vehicles

### Firm

The concept was revealed by IMI in 2006 and was expected to enter Israel Defense Forces tests by mid-2007. [1] It senses incoming threats via a fixed active electronically scanned array[1] radar sensor developed by RADA Electronic Industries and an optional passive infrared detector developed by Elbit's Elisra. [1]

### Technical Mean

When a threat is imminent, an explosive projectile interceptor is launched towards it. The interceptor explodes very near the threat, destroying or deflecting and destabilizing it by detonating its warhead. For this, only the blast effect of the explosive is used. The interceptor casing is made of combustible materials so minimal fragmentation is formed in the explosion, helping minimize collateral damage. [1] The system includes an electro-optic sensor suit, searching and tracking radar, and a reaction suit with launchers and interceptors, neutralizing threats at a safe distance from the APC. [2]

### Objectives

In basic terms, these armored protection systems use flat-panel radars and specialized optical systems to detect munitions fired at them - whether rounds from unguided rocket-propelled grenades like the ex-Soviet RPG or anti-tank missiles like Russian-made Kornet guided missile, both currently in use by Hamas. If a fast-moving projectile, like a missile, is fired at an APS-equipped vehicle, the systems can determine whether the projectile will hit the vehicle or not. If it appears to be on-target, the APS instantly fires one of several kinds of interceptor projectiles or "soft-kill" directed-energy (lasers) fire at the inbound missile, blowing it up in midair. The whole sequence happens in seconds, as illustrated by this video of Elbit's Iron Fist in action. [4]

### Target

Given that one of the first units to train on the Eitan is the 50th Battalion's Sayeret

Nahal, an elite unit within the brigade, the Iron Fist-equipped personnel carriers will likely soon be in action as IDF forces push into Gaza. [3]

## Effects

APS systems in use by the IDF's armored and infantry brigades may yield a trio of beneficial impacts on the battlefield: fewer armored personnel carriers and tanks will be damaged or destroyed by Hamas fire, less likely to cause unintended non-combatant Palestinian casualties in the confines of Gaza streets, and missile launcher teams and RPG-wielding fighters are more likely to be silenced and taken out of action. Even if the APS on IDF Eitans, Merkavas and other ground armor isn't perfect, Israel will surely place equipped vehicles squarely in the fight in Gaza while keeping an eye northward to the Lebanon border where the threat of rocket and missile fire is exponentially greater. [4]

## Sources

[1] [https://en.wikipedia.org/wiki/Iron\\_Fist\\_\(countermeasure\)](https://en.wikipedia.org/wiki/Iron_Fist_(countermeasure)) [2] <https://www.israeldefense.co.il/en/node/56600> [3] <https://www.forbes.com/sites/erictegler/2023/10/20/active-protection-systems-for-armor-could-change-the-fight-in-gaza/> [4] <https://www.forbes.com/sites/erictegler/2023/10/20/active-protection-systems-for-armor-could-change-the-fight-in-gaza/>

## Drones

## Elbit Systems

UAV Hermes 450, 900, ... / Iron Sting / ...

### Firm

- \* Elbit Systems developed the Hermes 450 unmanned aerial vehicle (UAV) being used in Gaza
- \* The infamous Israeli-made Galil rifles, once used in the Guatemalan genocide, ended up with Colombian drug lords in the late 1980s. ... American and Colombian investigators discovered that the weapons were part of a murky deal between Israeli mercenaries and Medellín cocaine cartel head Jose Gonzalo Rodriguez Gacha when he wanted to take over the country and build a neofascist state. [2. p47]
- \* Israeli technology was sold as the solution to unwanted populations at the US-Mexico border where the Israeli company Elbit was a major player in repelling migrants [2, p50]
- \* Working closely with Microsoft engineers, Elbit Systems redesigned the architecture of the OneSim™ infrastructure to meet the requirements of cloud solutions and upload the OneSim™ to the Microsoft Azure cloud. OneSim™ is Elbit Systems' platform-agnostic simulation software infrastructure that provides land, air and marine users a complete solution for training systems, from a stand-alone simulator and up to multi-platform Mission Training Centers. [3]
- \* C4I and Cyber. Headquartered in Netanya, Israel, Elbit Systems C4I and Cyber Ltd. (C4I and Cyber) is engaged in the worldwide market for C4ISR systems, data links and radio communication systems and equipment, cyber intelligence solutions, autonomous solutions and homeland security solutions. Elisra. Based in Holon, Israel, Elbit Systems EW and SIGINT – Elisra Ltd. (Elisra) provides a wide range of electronic warfare (EW) systems, signal intelligence (SIGINT) systems and C4ISR technological solutions for the worldwide market. Elop. Based in Rehovot, Israel, Elbit Systems Electro-Optics Elop Ltd. (Elop) designs, engineers, manufactures and supports a wide range of electro-optic and laser systems and products mainly for defense, space and homeland security applications for customers worldwide. ELS. Headquartered in Ramat HaSharon, Israel, Elbit Systems Land Ltd. (ELS) is engaged in the design and manufacture of land-based systems and products for armored and other military vehicles, artillery and mortar systems. IMI. Headquartered in Ramat HaSharon, Israel, IMI Systems Ltd. (IMI) is engaged in the design and manufacture of a wide range of precision munitions for land, air and sea applications and guided rocket systems, as well as armored vehicle and other platforms survivability and protection systems for defense and homeland security applications. ##### Technical Mean
- \* major activities include: military aircraft and helicopter systems; commercial aviation systems and aerostructures; unmanned aircraft systems (UAS); electro-optic, night vision and countermeasures systems; naval systems; land vehicle systems; munitions ;



command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) and cyber systems; electronic warfare and signal intelligence systems; and other commercial activities. [4]

## Effects

\* an Israeli Spike drone rocket ... can be modified to carry a fragmentation sleeve of thousands of 3mm tungsten cubes, said to affect an area of approximately 20 metres in diameter. The cubes puncture metal and “cause tissue to be torn from flesh”, literally shredding anyone within range, according to Erik Fosse, a Norwegian doctor working in Gaza. [5]

## Sources

\* [1] <https://www.bbc.com/news/world-middle-east-68737412>

\* [2] Antony Loewenstein - The palestine laboratory (2023)

\* [3] <https://elbitsystems.com/pr-new/elbit-systems-simulation-infrastructure-becomes-cloud-native/>

\* [4] <https://elbitsystems.com/about-us-introduction/>

\* [5] <https://www.aljazeera.com/features/2023/11/17/israels-weapons-industry-is-the-gaza-war-its-latest-test-lab>

## Israel Aerospace Industries

IAI Heron (Machatz-1) / Super Heron / IAI Eitan / Jaguar / REX MKII

Firm

Israel Aerospace Industries (Hebrew: התעשייה האווירית לישראל, romanized: ha-ta'asiya ha-avirit le-yisra'el), is Israel's major aerospace and aviation manufacturer, producing aerial and astronautic systems for both military and civilian usage. It has 14,000 employees as of 2021. IAI is state-owned by the government of Israel. [2] Israel Aerospace Industries has received EU funding via 29 projects. The EU's ambassador in Tel Aviv has congratulated Israeli partners in EU collaborative projects, such as Israel Aerospace Industries for 'developing the aircraft of the future'. This is a euphemism for the company manufacturing the Heron drone, which has been used in attacks on Gaza (Cronin, 2018).[6] "Brochures for the Heron describe it as "combat proven." Bureaucrats in Brussels have not been perturbed by that creepy euphemism. They have approved the participation of Israel Aerospace Industries in Horizon 2020, the EU's latest research program. At least one of the grants which the firm has received through that program is for work focused on drone technology." [7] The University of Patras (Greece) has 13 joint projects with IAI, while the University of Stuttgart (Germany) and Delft Technical University (the Netherlands) both participate in nine projects with IAI [10] ##### Technical Mean The Heron navigates using an internal GPS navigation device, and either a pre-programmed flight profile (in which case the system is fully autonomous from takeoff to landing), manual override from a ground control station, or a combination of both. It can autonomously return to base and land in case of lost communication with the ground station. The system has fully automatic launch and recovery (ALR) and all-weather capabilities.[1] The Jaguar is equipped with a 7.62 mm MAG machine gun which can operate while stationary or on the move. The robot utilizes high-resolution cameras, transmitters, powerful headlights, and a remote-controlled PA system. Additionally, it has the ability to self-destruct if it falls into enemy hands. The most unique aspect of the Jaguar is its semi-autonomous system. The robot is capable of driving by itself to a predetermined destination while spotting and bypassing obstacles using sensors and an advanced driving system, all while its operators and commanders have full operational control. [9] REX MKII is operated by an electronic tablet and can be equipped with two machine guns, cameras and sensors, said Rani Avni, deputy head of the company's autonomous systems division. The robot can gather intelligence for ground troops, carry injured soldiers and supplies in and out of battle, and strike nearby targets [8]

## Objectives

Along with intelligence, surveillance, target acquisition, and reconnaissance (ISTR), Israeli IAI Eitan ... capable of holding armed roles. All exports of the aircraft are unarmed. [3]

## Target

Heron UAS and Heron TP drones in the service of the Israeli Air Force have been actively deployed in the ongoing war with the Palestinian Hamas movement since October 7, the beginning of the Hamas attack on the Jewish state. As early as a few minutes after 7 a.m. on that seventh day of October, Heron family drones were already gathering intelligence for the IDF and providing cross-command communications and situational awareness. Thanks in part to the timely deployment of these assets, Israeli soldiers were able to quickly dislodge the terrorists from their territory. [4] With a significantly long endurance per operational mission, Heron and Heron TP platforms currently perform 24/7 surveillance sorties, each spanning over days. Operators are replaced with fresh teams every few hours, thus maintaining high alert without leaving the target area on rotations. [5]

## Effects

“The Heron will continue to safeguard Israel, deliver intelligence deep inside hostile areas, and reveal the enemy anywhere and anytime.” This is the time to fight with full, aggressive power! Seek and destroy the enemy,” Squadron Commander Col. F wrote in his combat address.” [5] “With every mission, the device collects more data which it then learns from for future missions,” said Yonni Gedj, an operational expert in the company’s robotics division. [8]

## Sources

[1] [https://en.wikipedia.org/wiki/IAI\\_Heron](https://en.wikipedia.org/wiki/IAI_Heron) [2] [https://en.wikipedia.org/wiki/Israel\\_Aerospace\\_Industries](https://en.wikipedia.org/wiki/Israel_Aerospace_Industries) [3] [https://en.wikipedia.org/wiki/IAI\\_Eitan](https://en.wikipedia.org/wiki/IAI_Eitan) [4] <https://www.defensemagazine.com/article/israel-in-gaza-demonstrates-the-widespread-use-of-drones-on-the-modern-battlefield> [5] <https://www.iai.co.il/news-media/iai-action/IAI-Unmanned-Aerial-Dominance> [6] <https://www.eccpalestine.org/beyond-dual-use-israeli-universities-role-in-the-military-security-industrial-complex/> [7] <https://electronicintifada.net/blogs/david-cronin/eu-funds-israels-war-industry> [8] <https://apnews.com/article/technology-middle-east-business->

israel-628f878f704b7c082ec2ebc9e9441173 [9] <https://www.israeldefense.co.il/en/node/49744> [10] [Partners in Crime; EU complicity in Israel's genocide in Gaza](#)  
Transnational Institute - 4 June 2024

## Rooster

Robotican's New Hybrid Robotic Drone

Firm

The drone is manufactured by the Israeli company Robotican, a developer and manufacturer of autonomous robots and drone systems.

Technical Mean

The Rooster boasts up to 15 minutes of flying time and 40 minutes of rolling time, with an average working time of up to 90 minutes. The drone effortlessly transitions between flying in the air and rolling on the ground, ensuring adaptability to any terrain.

[1] The Rooster can be customized with a range of payloads, such as thermal cameras, gas sensors, and radiation sensors, adapting to multiple mission requirements. [1]

Sources

[1] <https://www.israeldefense.co.il/en/node/60981>

## **ROBUST, the acronym for ROBotic aUtonomous Sense and strike**

### Firm

it has been developed by the Israeli Ministry's Directorate of Defense Research and Development (DDR&D), the Tank and APC Directorate, and Israeli defence industries, among which BL Advanced Ground Support Systems Ltd. and Elbit Systems

### Technical Mean

The Medium Robotic Combat Vehicle (M-RCV) is a 6×6 wheeled vehicle of considerable dimensions, as its rear ramp might well allow infantrymen to enter the vehicle, but it is meant to remain a fully unmanned system. The chassis was developed by BL and is named BLR-2; the vehicle has no steering axles, steering being obtained by the differential speed on the various wheels. This steering system allows pivot turning, reducing to nil the turning radius, a considerable advantage especially when operating in reduced spaces such as woods or dense urban areas. Coming to lethality, the ROBUST was fitted with the MATE 30 unmanned turret, armed with the Mk44 30 mm Northrop Grumman cannon and a 7.62 mm coaxial machine gun. Developed by the Tank and APC Directorate for the Eitan 8×8 infantry fighting vehicle, according to information the main armament maximum elevation is 70°, which fits well possible urban engagements. The "virtual gunner" is fitted with autonomous target recognition, auto-tracking for multiple targets, smart fire plan and context-based target prioritisation.

### Sources

[1] <https://www.edrmagazine.eu/a-robust-combat-unmanned-vehicle-from-israel>

## HERO loitering systems

HERO is a sensor-to-shooter system used for surveillance, target acquisition and attack of a variety of targets. The family of loitering systems supports several launch methods: from the ground by a single soldier, from a vehicle, and from a variety of aerial and naval platforms. The HERO flies to the target area, loiters above the point of interest, tracks, and attacks the target.[1]

### Firm

UVision Air Ltd. is an Israeli defense technology company established in 2011. [1]

### Technical Mean

It is operated remotely and controlled in real time by a communications system. The HERO is equipped with an electro-optical camera whose images are received by the command and control station.[1]

### Objectives

This forms a very rapid sensor to shooter cycle,” Uvision CEO Major General (ret) Avi Mizrahi told Janes . “There is no need for someone to acquire a target, punch in 10 coordinate digits, and send the target data onwards. A soldier in a vehicle sees a target and strikes.” The cannister-launched munition produces no smoke or fire, so does not give away the position of its operators. “Hence, special forces like it,” Mizrahi said. [2]

### Target

The Hero-30 is designed to enable frontline troops to carry out precision strikes against enemy personnel or light vehicles. [2]

### Effects

Ensuring minimal logistics and simplified setup and deployment procedures, the Hero-90 is lightweight, easily carried and operated by the dismounted soldier, and can be launched in less than two minutes. Designed to bring unprecedented lethality [3]

### Sources

[1] [https://en.wikipedia.org/wiki/UVision\\_Air](https://en.wikipedia.org/wiki/UVision_Air) [2] <https://www.janes.com/defence->

news/news-detail/idf-using-uvision-mini-loitering-munition [3] <https://unmanned-network.com/uvision-air-launches-revolutionary-hero-90-a-portable-tactical-loitering-munition-system-with-anti-strike-capabilities-for-dismounted-soldiers/>



## **Aeronautics**

SkyStar surveillance balloons / Aerostar UAV / Pegasus 120" VTOL UAV (Chocolate Milk Drone', Hebrew: Shoko Drone)

### Firm

Aeronautics: an Israeli company that develop, manufactures and markets Unmanned Aerial vehicles (UAV) and aerial intelligence and surveillance systems for governments, military and civil entities. (subsidiaries: Controp Precision Technologies, RT LTA Systems) Aeronautics, jointly with Motorola, developed the "Stronghold" surveillance technology that includes radars and cameras, the technology is installed in dozens of settlements in the West Bank.

### Sources

<https://www.whoprofits.org/companies/company/3997?aeronautics#>

## Research & Development

## **MAFAT / Directorate of Defense, Research, & Development (IMOD DDR&D or DDR&D)**

Israel's Administration for the Development of Weapons and Technological Infrastructure, the R&D directorate of Israel's Ministry of Defence [1, p 107] ##### Firm - a joint administrative body of the Israel Ministry of Defense (IMOD) and the Israel Defense Force (IDF) [2] - cooperates with the IMOD and the IDF, defense companies such as IMI Systems, Israel Aerospace Industries, Rafael Advanced Defense Systems, Elbit Systems, the Institute for Biological Research, the Israel Space Agency, startups, academic institutions, and more [2] ##### Technical Mean - The Military Research and Development Unit is charged with initiating and leading technological research and development [2] - The Science and Technology Unit is responsible for defense related technological infrastructure and applied scientific research. [2] - The IMDO (Israel Missile Defense Organization) is responsible for the R&D and equipment of active defense systems such as the Iron Dome, David's Sling, Arrow-2 and Arrow-3, as well as detection and warning systems such as Sky Dew. The IMDO works in cooperation with the American Missile Defense Agency (MDA), on joint ventures and the development of defense systems. [2] - The UAV Administration is responsible for managing the unmanned aircraft systems for Israeli security forces [2] - The Space and Satellite Administration coordinates all of Israel's aerospace defense activities [2] ##### Objectives MAFAT's stated aim is to 'ensure Israel's ability to develop weapons to build its strength and to continue to maintain its qualitative advantage. MAFAT is therefore responsible for weapons and technology infrastructure, cultivating technological research personnel, soliciting and funding research from Israeli universities, and collaborating with academic institutions and military industries on development for the Israeli military. [1, p 107] ##### Target the development of innovative concepts for defense technology, managing the Israel Ministry of Defense's short and long term projects relating to defensive technology, serving as a professional technical body for the research and development of military and defensive technology, cooperating with international partners in the field of research and development [2] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] [https://en.wikipedia.org/wiki/Directorate\\_of\\_Defence\\_Research\\_%26\\_Development](https://en.wikipedia.org/wiki/Directorate_of_Defence_Research_%26_Development)

## Horizon 2020 (EU research program)

Horizon 2020 and Horizon Europe are research cooperation funding programs in which European universities cooperate with Israeli entities ##### Firm – Israel’s police and its public security ministry are among the participants in Roxanne. [1] – partners Roxanne include Airbus, Universitat des Saarlandes, Capgemini, Leibniz University Hannover, Netherlands Forensic Institute, Aegis IT Research, and others. [4] – partners POLIICE include Libereu (Israel), Nokia, Privanova, Rohde & Schwarz, Universidad Politecnica Madrid, KPMG, Elektron, Bae Systems ##### Technical Mean – under the Horizon Europe programme there is one project that involves an Israeli entity that works alongside the Israeli military conducting ‘war games and simulations’. This project, titled EU-GLOCTER, is worth a total of €2.6 million and is coordinated by Dublin City University in Ireland involving a collaboration with various partners including Israel’s Reichman University and Counter-Terrorism Solutions Ltd. Other projects are similarly problematic and involve funding for surveillance, digital advances and technology – this at a time when Israel is waging a war that is highly dependent on high-tech digital war tools.[6] – POLIICE, which “aims to advance European law enforcement agencies (LEAs) to novel LI, investigation and intelligence methods that can effectively investigate crime and terrorism”. [1] – POLIICE will research and model quantum unlock, detection, and decryption as a service to improve information exchange and cooperation between European LEAs [5] – The EU-funded ROXANNE project intends to combine new speech technologies, face recognition and network analysis to facilitate the identification of criminals. Specifically, ROXANNE will develop a platform that will increase agencies’ capabilities via voice recognition, language and video technologies. [1] – ROXANNE focused on privacy-aware criminal network analysis enhanced by AI technologies supporting multilinguality (specifically EU languages) and multimodality (speech, text, video, metadata) to provide LEAs with an efficient legal framework and technical tools to track and uncover criminal identities [3] ##### Objectives – The advent of new communication technologies such as 5G & beyond, end-to-end encrypted communication, and quantum-based encryption has made traditional lawful interception (LI) solutions ineffective against crime and terrorism. To address this challenge, the EU-funded POLIICE project aims to advance European law enforcement agencies (LEAs) to novel LI, investigation and intelligence methods that can effectively investigate crime and terrorism. It will deliver, research, validate and demonstrate innovative LI measures at the cloud, network, and edge device levels [5] ##### Effects – The European Union funds research involving Israel’s police despite admitting that it may be used for spying purposes [2] – Internal EU documents obtained under freedom of information rules confirm there is a risk that Roxanne’s results will be used for mass surveillance. [2] ##### Sources [1] <https://>

stopwapenhandel.org/european-universities-cooperation-with-israel-in-eu-security-research-programs/ [2] <https://electronicintifada.net/blogs/david-cronin/eu-admits-teaming-israeli-police-enables-mass-surveillance> [3] <https://cordis.europa.eu/project/id/833635/reporting> [4] <https://cordis.europa.eu/project/id/833635> [5] <https://cordis.europa.eu/project/id/101073795> [6] [Partners in Crime; EU complicity in Israel's genocide in Gaza](#) Transnational Institute - 4 June 2024

## Universities

Universities have birthed, funded, and advanced their scientific research through the Israeli security state and Israeli weapons corporations. ... They offer their campuses, resources, students, and faculty to aid in the development of technology and weaponry deployed against Palestinians and then sold worldwide as 'battle-proven'. [1, p 111] IDF is deeply involved in all Israeli academic institutions, including eight universities and some twenty colleges. Most institutions employ ex-officers as administrators, and most presidents of Israeli academic institutions are retired senior officers. Academia is a racialized part of the apartheid machinery; it offers special deals and arrangements for IDF veterans, thus excluding most non-Jewish citizens. [2] High-level appointments have gone to 'individuals known to have supervised and designed repressive measures and persistently committed violations of international humanitarian law against Palestinians in their other careers as military and intelligence functionaries' (Taraki, 2015). Such individuals are treated as prestigious rather than as morally abject. [3] [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] Uri Yacobi Keller - Academic Boycott of Israel, in Economy of the Occupation (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf> [3] <https://www.eccpalestine.org/beyond-dual-use-israeli-universities-role-in-the-military-security-industrial-complex/>

## Technion

“Technion opened a Department of Aeronautical Engineering in 1954. The department tailored specialized courses based on Israeli military needs” [1, p92] ##### Firm - “its faculty and students spearheaded the development of Israeli Aerospace Industries (IAI), transforming it into a company that produced Israeli-designed and manufactured fighter jets and missiles” [1, p92] - in 2021, the Technion committed to developing new software for Rafael, Elbit, and Lockheed Martin [1, p107] ##### Technical Mean - Technion researchers have developed a wide range of technologies - including new missiles and drones - which have gone into production by Rafael, IAI, and other Israeli weapons corporations, and then gone on to be used by the Israeli military. [1, p92/93] - Technion runs Alonim, an accelerated BSc to MSc program in data science for soldiers, after which they are incorporated into R&D projects in technological military units and the security state [1, p 102] - Technion created a university-to-military-industry pipeline, bringing Israeli weapons corporations onto campus and building programming so as to integrate their students into the industry while they are still enrolled. Rafael routinely arrives on campus to solicit students as employees ... Elbit has granted hundreds of thousands of dollars to fund directed research grants and scholarship programs and also trains students and the advanced laboratory it installed on campus in electro-optics and other fields with military industry application. [1, p 106] - Alongside Ben-Gurion University, the Technion offers the Brakim BSc to MSc program in engineering, training soldiers for R&D in Israel’s military and military industries. The accompanying Bareket master’s program in data engineering, run with Bar-Ilan University, trains soldiers in data science, coding, and programming for military application. [1, p102] - The Technion not only facilitated the birth of the Israeli military industry but also continues to support the international sales of its weaponry, even going so far to explicitly offer courses on arms and security marketing and export. [1, p110] - The Haifa Technion helped to develop the D9 remote-controlled bulldozer, widely deployed in the destruction of Palestinian homes. During 2008-2013 it had a research partnership with Elbit Systems Ltd. ... Bar-Ilan University has participated in joint research with the army, specifically in developing artificial intelligence for unmanned combat vehicles...Technion University has become virtually the R&D wing of the Israeli military. ... Technion has manufactured technologies specifically to torment recalcitrant populations. [2] - Elbit Systems grants half a million dollars to the Technion in research grants. [3] - Technion has a policy of full cooperation with “homeland security” projects such as unmanned vehicles.[3] - Technion researchers develop unmanned vehicles that also aid the Israeli army in destroying Palestinian houses.[3] - Technion researchers developed a method for discovering underground tunnels, aimed specifically at aiding the siege on Gaza. [3] -

Technion and Elbit Systems found a joint research center. [3] – Technion researchers developed unmanned land vehicles for Israeli military use [3] ##### Objectives “Since the establishment of these military industries, they have remained embedded in the Technion and are often difficult to distinguish from the university. Scientists and engineers regularly moved back and forth between the university and the weapons companies and have sent their students to join them as employees. The companies, for their part, have funded the establishment of major Technion laboratories, and a network of Technion faculty dedicated to military research and development have functioned as their shadow employees.” [1, p92] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] <https://www.eccpalestine.org/beyond-dual-use-israeli-universities-role-in-the-military-security-industrial-complex/> [3] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>



## Hebrew University

Hebrew University was the Zionist movement's first comprehensive university dedicated to research and teaching across disciplines. [1, p90] ##### Firm Hebrew University's commercialization companies have formed long-term partnerships with Israeli and international military industries. Hebrew University's commercialization company, Yissum ('application' in Hebrew), currently claims status as a global leader in technologies used for 'homeland security'. The US Government invests millions of dollars annually in supporting Hebrew University's 'counter-terrorism' research and Yissum's technologies acquisition. [1, p 109] ##### Technical Means - Hebrew University's Talpiot combined BSc in physics, computer science, and math. Under the auspices of the Administration for the Development of Weapons and Technological Infrastructure and the Israeli Air Force, the program fosters leadership in 'technological research' for the maintenance and development of weapon systems for the Israeli military and the security establishment. [1, p 101] - Hebrew University Mt. Scopus is policed particularly vigilantly by the administration and campus security. Palestinian students describe in interviews how they are alienated by the university prohibitions on clothing and other items expressing their identity [1, p150] - All military colleges and training facilities, including the military "Command and Staff College" which trains officers, are under the academic auspices and responsibility of the Hebrew University. [2] - One of the Hebrew University's campuses has expanded into the Occupied Territories in a confiscation of Palestinian land. In addition, some of the university owned student quarters are located in a settlement neighborhood of Jerusalem. [2] ##### Objectives ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>

## University of Haifa

Firm

At the University of Haifa, the Comper Interdisciplinary Center for the Study of Anti-Semitism and Racism plays another role in Israel's hasbara, primarily by mobilizing students. "Ambassador Online", a program initiated and led by center head and media studies professor Eli Avraham, offers academic and 'practical training' to cultivate student capabilities to become 'unofficial ambassadors' and leaders in Israel's hasbara. [1, p 96] "The university of Haifa is responsible for the academic training of the IDF's command core for years to come" (Prof Ron Rubin, former president of the University of Haifa, quoted in 1, p99) ##### Technical Mean - As shown by previous syllabi, the [Ambassador Online] course content includes lectures by University of Haifa faculty and deans, alongside members of the Israeli state hasbara apparatuses, including from the Prime Minister's Office and the Ministry of foreign affairs. The course final assignment was to create content for Israeli public diplomacy. [1, p96/97] - the University of Haifa offers a tailored master's degree in security theory for Israeli colonels and high-ranking members of Israeli security agencies. [1, p 100] - through the Alon Command and Control college, the University of Haifa offers the first tailored master's degrees in political science to army battalion commanders and air force squadron commanders, with a specialization in 'military security'. [1, p101] - The University's department for Geo-strategy takes pride in helping shape Israeli "demographic" and security policies. [2] - Haifa University hosted a conference on the solution of the "demographic problem," another way of saying there are too many Palestinians in Israel. [2] ##### Objectives "Ambassadors Online" is designed to repress the BDS movement, in Israel and globally. [1, p98] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>

## Tel Aviv University

Hebrew University was the Zionist movement's first comprehensive university dedicated to research and teaching across disciplines. [1, p90] ##### Firm #####

Technical Mean - What the UN deemed war crime, the Institute for National Security Studies (INSS) at Tel Aviv University considered a public relations crisis. As early as June 2018, the INSS collaborated with the Israeli Military Spokesperson Unit to host a conference titled 'the battle for Public Opinion: Gaza as a Case Study'. The conference brought together military experts, officials from the Ministry of Foreign Affairs, journalists, and INSS fellows to discuss how Israel could best spin reports of Israeli public relations problems, with panelists lamenting the inferiority of the Israeli narrative in the international arena ... explicitly strategized about countering criticisms of Israel's military occupation and facilitating international identification with Israel. [1, p94/95] - INSS researchers regularly formulate policy for the Israeli state to combat the BDS movement and other campaigns critical of Israel, including the recommendation to employ Israeli intelligence agencies to 'incriminate', 'undermine', and 'sabotage' activists working for Palestinian rights. [1, p96] - Yuval Ne'eman Workshop for Science, Technology, and Security, ... leads academic research with concrete applications for the security state, including cybersecurity, robotics, missiles, and guided weapons. The workshop also holds a conference series at Tel Aviv University that includes members of the Israeli military and security agencies as well as Israeli and international military industries. [1, p107/108] Tel Aviv University's Center for Nanoscience and Nanotechnology, for example, collaborates on R&D with Israeli weapons companies, including IAI and Elbit. - Tel-Aviv University hosts a convention about weapons' development for the Israeli army [2] - The University appointed a military colonel whose military past includes overseeing and approving military attacks on civilians during the 2008 Gaza attacks, to a lecturer on international law [2] ##### Objectives the stated mission of the INSS is to conduct research on - and offer the Israeli government analyses and recommendations about - issues central to the state's 'national security agenda'. ... [1, p95] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>

## The Weizman institute

the Weizmann Institute was committed to scientific research for state-building. [1, p90] ##### Firm Senior administrators and faculty at the Weizmann Institute and the Technion later led the development of Israeli military industries. They advocated establishing Israeli science as the basis of Israeli military power by developing and manufacturing Israeli advanced weaponry. [1, p91] Weizman Institute and Elbit Systems cooperate to create a joint program. [2] ##### Technical Mean - The Weizmann Institute operates Kiryat Weizmann, a high-tech science park adjacent to its campus that facilitates joint research and product development between the institute and private corporations. It houses facilities of Israel's weapons companies Rafael and Elbit and Elbit's subsidiary El-Op's facilities at the park, works on technology for detecting targets illicitly photographed by drones, developed by the Weizman Institute and Ben-Gurion University. [1, p109] - Weizman Institute-sponsored company develops lubricants for the use of the Israeli military [2] ##### Objectives "By the end of the war, the Weizmann Institute had come to anchor the Military Science Corps and, together with Technion, became the military-scientific center of the Israeli state. The 1948 war marked the beginning, not the end, of university militarization. [1, p91] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>

## Ben-Gurion University

Firm

Ben-Gurion University's commercialization company, BGN Technologies, operates joint research and cooperation with Rafael, Elbit, IAI, and Lockheed-Martin. [1, p 110] ##### Technical Means ##### Objectives - Ben Gurion University initiated the idea for a "military medicine school" and appealed when the project was given to the Hebrew University [2] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>

## Bar-Ilan University

### Firm

Bar-Ilan University's commercialization company – BIRAD – operates a long-term partnership with Rafael and has facilitated a research collaboration with Elbit's technological incubator. Meetings between the technology team at Elbit and university researchers are intended to expose weapon developers to academic research 'on the verge of implementation'. This collaboration is critical to Israeli military industries, as Elbit's chief scientist made clear [1, p110] ##### Technical Means ##### Objectives - Bar Ilan University – Bar Ilan computer science researchers develop unmanned vehicle algorithms for Israeli military use. [2] ##### Sources [1] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024) [2] The Economy of the Occupation - Uri Keller (2009) <https://bdsmovement.net/files/2011/02/EOO23-24-Web.pdf>

## Surveillance

## Mabat 2000 / SMART M / SAIP / OSCAR

Mabat 2000 consists of hundreds of cameras in Jerusalem's Old City, a flashpoint of tensions in the occupied area. The solutions are based on Smart-M, an IoT-management platform developed by MER. By integrating sensory outputs and other types of data from various sources into a single interconnected management platform, Smart-M functions as the heart of the municipality's command & control center, providing complete visibility and enabling fast and efficient response. Smart-M has been operational for over 20 years and is constantly updated in correlation with advancing technologies. [3] Open Source Collection Analysis and Response, known as OSCAR, which trawls through the internet and social media platforms and promises to uncover hidden connections from the data OSCAR collects. Strategic Actionable Intelligence Platform, or SAIP, takes that data in and groups it together. To pinpoint "actionable intelligence," SAIP uses technology that can highlight words, sentences, and information that might interest intelligence officers. These types of language analysis tools are increasingly popular with intelligence services around the world as a tool for pinpointing the next threat.

### Firm

Mer Security is one of the companies exporting spy products. It is well-known in the country's security circles; it won an Israeli police contract in 1999 to establish "Mabat 2000." In an interview with the Israel Gateway magazine, a trade publication, Haim Mer, chairman of the company's board and also a Unit 8200 veteran, explained that "the police needed a system in which 'Big Brother' would control and would allow for an overall view of events in the Old City area." [1] The company's CEO, Nir Lempert, is a 22-year veteran of Unit 8200, the Israeli intelligence unit often compared to the National Security Agency, and is chairman of the unit's alumni association. [1] MER conceived and implemented Mabat 2000, an integrated command & control system that utilizes innovative security and communications technologies, tailored to the unique needs of the Old City. Since then, for over 23 years, Mabat 2000 has been operating 24 hours a day, 365 days a year, with MER regularly providing maintenance services and technological upgrades to meet the evolving security and safety needs. This world-leading cutting-edge command & control system has helped local security authorities maintain order in mass events in the Old City and has contributed to a major decline in criminal activities. [2]

### Technical Mean



another feature of SAIP: Users can create an avatar “in order to get the credentials to closed forums and to gather information from closed forums.

#### Sources

[1] <https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/> [2] <https://mer-group.com/fulfilling-a-popes-wish/> [3] <https://mer-group.com/solutions/safe-and-smart-cities/>

## Mispar Hazak

Firm

IDF / Unit 9900 / Tayeset 100

Technical Mean

“While specific technical details of “Mispar Hazak” might be classified, it likely involves a combination of advanced sensing technologies. These could include seismic sensors, acoustic sensors, and ground-penetrating radar (GPR), which are commonly used in subterranean detection. ... The effectiveness of “Mispar Hazak” is enhanced when integrated with other intelligence and surveillance systems, such as drones, satellites, and on-ground intelligence. ” “Future developments might involve the integration of artificial intelligence (AI) and machine learning algorithms to enhance the data analysis capabilities of systems like “Mispar Hazak”. AI can process vast amounts of sensor data more efficiently, identifying patterns and anomalies that indicate tunneling activities.”[1]

Objectives

“The system involves placing geophones, devices that measure energy waves in the earth, 1.5 meters into the ground. The geophones are equipped with acoustic components taken from sensors used by the navy and devices used in searching for oil. The system has passed initial tests and will be operational by late 2023” [2]

Target

“The primary function of the “Mispar Hazak” system is to locate underground tunnels. These tunnels, often used by militant groups for smuggling and launching attacks, pose a significant security challenge. The sensor system is designed to detect these structures and aid in their destruction, thereby neutralizing potential threats.” [1]

Effects

“The tunnels have been a lifeline for the people of Gaza who face a blockade by Israel and Egypt, a shortage of basic goods and services. The tunnels allow the transportation of food, medicine, fuel, construction material and even animals and vehicles.” [2]

## Sources

[1] <https://debuglies.com/2024/01/10/sophisticated-surveillance-systems-in-israel-for-tunnel-detection-in-the-gaza-strip-an-in-depth-analysis/> [2] <https://www.eurasiareview.com/10112023-fighting-underground-the-methods-and-technologies-of-the-gaza-tunnel-war-oped/>

## Palantir Technologies

Palantir Gotham / Palantir Apollo / Palantir Artificial Intelligence Platform (AIP) / TITAN

### Firm

Palantir Technologies - Palantir Technologies Inc. is a public American company that specializes in software platforms for big data analytics. [1] - provides the Israel Defence Force (IDF) with intelligence and surveillance services, including a form of predictive policing. In January 2024, Palantir agreed to a strategic partnership with the IDF under which it will provide the IDF with services to assist its “war-related missions”. [1]

### Technical Mean

- \* Palantir Artificial Intelligence Platform (AIP) is meant to run large language models like GPT-4 and alternatives on private networks. In one of its pitch videos, Palantir demos how a military might use AIP to fight a war. In the video, the operator uses a ChatGPT-style chatbot to order drone reconnaissance, generate several plans of attack, and organize the jamming of enemy communications. [2]
- \* The company is currently developing an even more powerful AI targeting system called TITAN (for “Tactical Intelligence Targeting Access Node”). According to Palantir, TITAN is a “next-generation Intelligence, Surveillance, and Reconnaissance ground station enabled by Artificial Intelligence and Machine Learning to process data received from Space, High Altitude, Aerial and Terrestrial layers.” Although designed for use by the US Army, it’s possible that the company could test prototypes against Palestinians in Gaza. [3]

### Objectives

- \* As one of the world’s most advanced data-mining companies, with ties to the CIA, Palantir’s “work” was supplying Israel’s military and intelligence agencies with advanced and powerful targeting capabilities [3]

### Target

- \* The project involved selling the ministry an Artificial Intelligence Platform that uses reams of classified intelligence reports to make life-or-death determinations about which targets to attack. [3]

## Effects

- \* allow Israel to “place three drone-fired missiles into three clearly marked aid vehicles.”  
[3]

## Sources

- \* [1] [https://en.wikipedia.org/wiki/Palantir\\_Technologies](https://en.wikipedia.org/wiki/Palantir_Technologies)
- \* [2] <https://www.vice.com/en/article/qjvb4x/palantir-demos-ai-to-fight-wars-but-says-it-will-be-totally-ethical-dont-worry-about-it>
- \* [3] <https://www.thenation.com/article/world/nsa-palantir-israel-gaza-ai/>

## Basel System / Maoz System

Israeli authorities have set limitations on Palestinians who seek work in Israel, and have increased the role of technology in the checkpoints stationed within the OPT (Section 5.5). As part of this control mechanism, Israeli authorities have required Palestinians to carry biometric identity cards since 2005. The cards are managed through the “Basel system” [1] First the Basel system was deployed in Gaza and later in the West Bank. That system was followed by the Maoz system in 2004. In the immediate aftermath of the second intifada and onwards, the Israeli security apparatus has been developing its technological capabilities rapidly and paired it with extensive deployment and use of CCTV infrastructure in the OPT [3]

### Firm

HP has operated since October 1999 through its subsidiary EDS Israel. The contract was worth \$10 million. The company that was first selected to distribute magnetic cards to Palestinians was On Time Innovations Ltd. [1] ... in March 2017 HP struck gold when the Israeli Knesset approved the Biometric Database Law for the entire Israeli population, making biometric identity cards and passports obligatory, and giving HP the contract to produce those cards with tender exemption, worth about \$300 million [1]

### Objectives

The reason for implementing the Basel system, according to OTI CEO Oded Bashan, is “secured and easy personal identification of people during border crossing while minimizing unnecessary contact and friction” (ibid.). This quote is a reminder about the use of technology of control by Israeli authorities to minimize human involvement in security, and as a substitute for policy. Automated control also makes a statement that contact with the Palestinian population is a peripheral and secondary function of the Israeli security organizations, and therefore can be safely privatized. [1]

### Target

After the system of biometric identity cards had been implemented for Palestinians, the Israeli police became familiar with the system, and Israeli politicians suggested that use of the system could be expanded to include labor migrants in Israel [1]

### Sources

- [1] Hever, S. - The privatization of Israeli Security (2018) H6.5 [2] BIOMETRICS AND COUNTER-TERRORISM Case study of Israel/Palestine (2021) - [https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel\\_Palestine%20v7.pdf](https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel_Palestine%20v7.pdf)
- [3] AUTOMATED APARTHEID (2023) - <https://www.amnesty.org.uk/files/2023-05/Automated%20Apartheid.pdf?VersionId=hKRPWbz18UpH1w1kyx9RgbJoChyWKWxU>

## **PIBA (Israeli Population, Immigration and Border Authority)**

The system contains information collected through Israel's national population database and at the border and major checkpoints: personal information on the occupied Palestinian and Syrian people collected by Israel is stored and managed. ##### Firm IBM designed and operates the Eitan System of the Israeli Population, Immigration and Border Authority [PIBA] The Head of the Administration, Yaacov Ganot, was appointed in 2007. At the time, Knesset members and human rights groups expressed concern. Ganot had served as prisons commissioner and prior to that as head of the Immigration authority, where his employees were known for engaging in violent altercations with migrant workers. [2] ##### Technical Mean ##### Objectives ##### Target PIBA is also a part of Israel's permit system which requires Palestinians over the age of 16 to carry "smart" cards, containing their photograph, address, fingerprints and other biometric identifiers. Much like in apartheid South Africa's passport system, the cards double as permits which determine Palestinian rights to cross through Israeli checkpoints for any purpose, including work, family reunification, religious rituals or travelling abroad. ##### Effects ##### Sources [1] <https://www.aljazeera.com/opinions/2024/5/12/how-us-big-tech-supports-israels-ai-powered-genocide-and-apartheid> [2] [https://en.wikipedia.org/wiki/Population\\_and\\_Immigration\\_Authority](https://en.wikipedia.org/wiki/Population_and_Immigration_Authority)



## Aviv system

The Aviv system contains Israel's Population Registry which includes information on all Palestinians with Israeli citizenship and non-citizen Palestinian residents of occupied East Jerusalem. The system also documents all of the crossings under Israeli control, including Allenby Bridge Crossing, which is the only access for West Bank Palestinian residents to travel abroad; and Erez checkpoint, which is the only crossing for the movement of people between the besieged Gaza and Israel and the West Bank – both controlled by and subjected to Israeli authorities. Additionally, the system had a distinguished database that includes information on Israeli citizens who live in settlements in the occupied West Bank, under the name “Yesha database” (Hebrew acronym for the West Bank and Gaza).

### Firm

Hewlett Packard Enterprise Company (HPE) is an American multinational information technology provider. The Aviv system was established based on Itanium servers manufactured by HPE, with HPE's business partner DXC Technology which developed, operated and maintained the system. In May 2023, HPE was contracted by the Population and Immigration Authority to provide three Itanium servers for the Aviv System for NIS 3,829,410 from June 2023 until June 2026. In a response to an FOI submitted by Who Profits on April 7, 2021, the Israeli Population and Immigration Authority confirmed that the Aviv System is gradually being phased out and will be terminated in the coming years, following the takeover of the computerizing systems of the ministry by IBM.

### Sources

<https://www.whoprofits.org/companies/company/3774?hewlett-packard-enterprise-hpe>

## Meitar system

Meitar system is used by the Israeli Civil Administration to issue biometric ID cards to Palestinians for use in checkpoints in the West Bank. The cards are issued in three checkpoints in Qalandia, Tarqumiyah and Sha'ar Ephraim. [1]

### Firm

- \* One Software won several tenders, in value of more than NIS 800,000, from the coordinator of government activities in the occupied territories, for IT consultant and management of “Meitar” system. The company’s subsidiary One Security Computing Projects Division, an authorized supplier to the Israeli Ministry of Defense, has carried out multiple projects in the field of intelligence and Cyber for the Israeli military, including the Intelligence Corps, ICT Division and the Israeli Air Force. [1]
- \* Polimil is a private Israeli company that provides identification solutions and identification personal and smart cards. The company is providing biometric smart cards, printers, and additional equipment and services for the Israeli Civil Administration (ICA) [3]
- \* In 2018, Afcon’s subsidiary DM (3000) Engineering Ltd., provided screens for reception halls and queue management systems for the Meitar System in checkpoints as part of biometric project for NIS 43,742. The Meitar system is used by the Israeli Civil Administration to issue biometric ID cards to Palestinians for use to cross Israeli checkpoints in the West Bank. The cards contain personal identifying information and are part of the identification technology array used by the Israeli military in checkpoints [2]

### Objectives

The biometric cards contain identifying information that is being stored in “Rolling Stone” system, a population registration system of Palestinian population in the West Bank, operated by the ICT and Cyber unit of the Israeli military, and can be used for intelligence purposes. As of 2020, 600,000 biometric ID cards have been issued in Meitar system. The use of identification technology by the Israeli military in checkpoints is part of the deployment of surveillance practices and technologies used for population control and spatial monitoring of Palestinians by Israel. [1]

### Sources

[1] <https://www.whoprofits.org/companies/company/3649?one-software-technologies> [2] <https://whoprofits.org/companies/company/4146?afcon-holdings> [3] <https://www.whoprofits.org/companies/company/4048?polimil>

## A1 Munasq

### Firm

- \* Al Munasq is launched by Israel's Coordination of Government Activities in the Occupied Palestinian Territory unit (COGAT) [2]

### Technical Mean

-it combines personal information of the civil records, such as place and date of birth, information on the extended family, place of residence with military records, tracking movement. The app can access all information and data on any other application on the same phone, including location data, incoming and outgoing calls, messages and emails [2]

### Objectives

- \* during the pandemic, Israel last year launched a mobile application to replace in-person permitting services. ... Without proper permits, it can be difficult to find work within the small geographical areas to which many Palestinians are confined. [1]

### Target

- \* Israel's pandemic response has thus forced Palestinians to choose between access to a professional livelihood, or maintaining their right to privacy. [1]
- \* approximately 50,000 users have downloaded the application [june 2020], with a rise in downloads due to restrictions under the guise of Covid-19, which forced many Palestinian workers to seek permits [2]

### Effects

- \* While the app was framed as a public health measure, its more insidious intentions are clear in its terms of service, which force users to provide access to the data stored on their phones, such as calls and photos. This becomes more problematic when understanding how important these services are for many Palestinians.[1]
- \* Despite the fact that the application is providing Palestinians with necessary services, the application is also collecting private information about the user, including files, messages, location data and even information from the camera, as revealed by Israeli media. This information is then used by the Israeli security services to spy on, develop profiles of and track Palestinians. [2]

## Sources

\* [1] <https://www.middleeasteye.net/opinion/israel-palestine-surveillance-tech-dystopia>

\* [2] <https://7amleh.org/2020/06/14/the-palestinian-digital-rights-coalition-warns-against-the-phone-application-the-coordinator>

## Spyware

# Pegasus

## Firm

- \* NSO, founders Shulev Hulio and Omri Lavie (ook Q Cyber Technologies / OSY Technologies / Westbridge)

## Technical Mean

- \* When Pegasus is installed on a person's phone, an attacker has complete access to a phone's messages, emails, media, microphone, camera, passwords, voice calls on messaging apps, location data, calls and contacts. The spyware also has the potential to activate the phone camera and microphone, and spy on an individual's calls and activities. [1]

## Objectives

- \* NSO's signature technology, the Pegasus system, was engineered to invade and then take over a mobile phone in order to surveil the owner. This was military-grade, offensive weapon. [3, p192]
- \* NSO's push to help in the war effort comes amid a wide-reaching, U.S.-based lobbying campaign to loosen restrictions. [2]
- \* NSO insists its software and support services are licensed to sovereign states only, to be used for law enforcement and intelligence purposes. [3. p viii]

## Target

- \* Six Palestinian human rights defenders hacked with NSO Group's Pegasus Spyware [1]
- \* several Israeli agencies are likely using Pegasus – a “zero-click” malware that can be snuck onto a target's device without them knowing – to help track people kidnapped by Hamas, as well as people who have gone missing during Hamas' attack [2]

## Effects

- \* As such, the spyware not only allows for the surveillance of the target, but also anyone with whom they have contact via that device. This means that, in addition to the targeting of Palestinians, including dual nationals, non-Palestinians (including foreign nationals and diplomats) with whom these victims were in contact, including Israeli citizens, could have also been subject to this surveillance, which, in the case of its citizens, would amount to a breach of Israeli law. [1]

## Sources

- \* [1] <https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus>
- \* [2] <https://www.axios.com/2023/11/14/pegasus-nso-hamas-israel-spyware>
- \* [3] Laurent Richard & Sandrine Rigaud, 2013, Pegasus. The secret technology that Threatens the End of Privacy and Democracy.

## Sherlock / custom Candiru spyware

### Firm

Candiru / Grindavik Solutions / LDF Associates / Taveta / D.F. Associates / Greenwich Solutions / Tabatha / Saito Tech (latest name) is a technology company offering surveillance and cyberespionage technology founded by Eran Shorer and Yaakov Weizman - Insanet, founded in 2019, is owned by ex-military and national defense types. Its founders include the former chief of Israel's National Security Council Dani Arditi and cyber entrepreneurs Ariel Eisen and Roy Lemkin [2]

### Technical Mean

- \* Candiru has used mock website URLs made to appear like web addresses of NGOs, activist groups, health organisations, and news media organisations to ensnare targets [1]
- \* spyware for mobile platforms, servers, and cloud accounts. Candiru allegedly offers a range of target infiltration approaches, including infiltration through hyperlinks, man-in-the-middle attacks, weaponised files, physical attack, and a program called "Sherlock"
- \* Sherlock seems designed to use legal data collection and digital advertising technologies

### Objectives

- \* Sherlock that can infect devices via online adverts to snoop on targets and collect data about them for the biz's clients
- \* Sherlock seems designed to use legal data collection and digital advertising technologies [2]
- \* The purpose of such exploits is sinister, as it allows attackers to target victims based on their choice of news consumption, and implicitly their political leanings. It can also be used as a jumping-off point to narrow down further spyware attacks. [3]

### Target

- \* The findings indicated that Candiru's cyberespionage tools were being used to target civil society. Microsoft identified at least 100 targets that included politicians, human rights activists, journalists, academics, embassy workers, and political dissidents. Microsoft identified targets in multiple countries across Europe and Asia. [1]

### Effects



## Sources

- \* [1] [https://en.wikipedia.org/wiki/Candiru\\_\(spyware\\_company\)](https://en.wikipedia.org/wiki/Candiru_(spyware_company))
- \* [2] [https://www.theregister.com/2023/09/16/insanet\\_spyware/](https://www.theregister.com/2023/09/16/insanet_spyware/)
- \* [3] <https://www.middleeasteye.net/opinion/candiru-israel-spyware-surveillance-imperialism>

## Alien / Predator

- \* providing a variety of information stealing, surveillance and remote-access capabilities [1]

### Firm

Intellexa alliance. They include the Android spyware maker Cytrox, a little-known Macedonian start-up and the French 3G and 4G hacking specialist Nexa Technologies [1] Founder Tal Dillian spent 24 years in the Israel Defense Forces, first in an elite combat unit, where he learned the value of in-field surveillance tools that would become his stock-in-trade. Later he was made chief commander in the technological unit of the IDF's Intelligence Corps.

### Technical Mean

- \* includes recording audio from phone calls and VoIP apps; stealing data from Signal, WhatsApp and Telegram; and even hiding applications or preventing them from running after a device reboots. more technical details: <https://blog.talosintelligence.com/mercenary-intellexa-predator/>
- \* First, Alien is injected into the Zygote Android process from which applications are forked and launched. Once running within that special system process, it downloads the latest version of Predator as well as the app's communication and synchronization components. Alien can also create shared memory space for the stolen audio and data, and a SELinux context to help it bypass Android security features and avoid detection.

### Objectives

- \* Alongside Android hacking tools, there's tech that can recognize your face wherever you travel, listen in on your calls, and locate all the phones in an entire country within minutes, Dilian boasts. Every 15 minutes, he can know where you are, he says [2]

### Target

- \* designed to snoop on terrorists, drug cartels and the world's most egregious criminals. But that's not always the case. Politicians, human rights activists and journalists have been targeted too.[2]

### Sources

- \* [1] [https://www.theregister.com/2023/05/27/predator\\_analysis\\_talos/](https://www.theregister.com/2023/05/27/predator_analysis_talos/)

\* [2] <https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/#7f428ef231b7>

## Incarceration

## G4S security systems / G1 Secure Solutions

G4S provides security systems to Ketziot, Damon and Meggido prisons, as well as the Russian Compound (Al-Moskobiyeh) and Kishon (Al-Jalameh) detention and interrogation centers. G4S is responsible for these facilities' control and monitoring systems, in addition to visitation and CCTV systems. G4S also provides security systems and a central control room in Hasharon compound – Rimonim prison, which includes a wing for Palestinian political prisoners. [4] The company G1 was formerly part of the global G4S concern, which specializes in security personnel services, electronic security services, arrest alternative such as ankle monitors and operating private jail houses around the world.

### Allied Universal

G4S' parent company, Allied Universal, is said to have sold all its remaining business in apartheid Israel following years of campaigns waged by the BDS movement for Palestinian rights. G4S suffered serious "reputational damage" and lost lucrative investment contracts because of pro-Palestine activism. Several other human rights campaigns have also targeted G4S over what campaigners have said is the security firm's "long, violent record of human rights abuses against prisoners, migrants, and other communities worldwide, including the UK, South Africa and the US." [2] Last year another campaign group, War on Want, wrote to Bill Gates, the Microsoft founder, urging him to sell his stake in G4S because of its involvement in Israel. His charity, the Bill and Melinda Gates Foundation Trust, had bought 3.2 per cent of G4S through his investment group Cascade last June for £110m but reduced his stake to below 3 per cent last week. The Gates foundation declined to comment on the reasons behind the sale. [5]

### Technical Mean

The company provides 'security systems' such as access control, CCTV, intruder alarms, fire detection, video analytics and security and building systems integration technology, mobile security patrol and response services and alarm receiving and monitoring facilities, integrated facilities services for entire sites or estates for commercial customers and governments. G4S also provides electronic tagging and monitoring of offenders at home or in the community [1] In 2002 G4S bought the Israeli Hashmira security company, and merged it into the G4S group, thereby establishing a foothold in the Israeli security market during the height of the second Intifada. Through Hashmira, G4S gained the exclusive contract to operate a system of

surveillance of prisoners with electronic bracelets for NIS 30 million annually [3] - The company has provided equipment for Israeli-run checkpoints in the occupied West Bank and Gaza, including luggage scanning machines and full body scanners [6]

## Objectives

G4S promotes privatization of security in the world, and at the same time plans to take part in it and profit from it [3]

## Target

The prison holds 1,500 Palestinian political prisoners and includes a military court which judges detainees from the West bank on a daily basis. [6]

## Effects

For G4S, the participation in government contracts related to the control of Palestinians opens the door for G4S to operate in the Israeli private market as a security company. It also serves G4S in tenders for which it competes in other countries. [3] Al-Moskobiyyeh and Al-Jalameh centers, serviced by G4S, are renowned for their use of torture, including of children. For instance, in 2013, detainee Arafat Jaradat died as a result of torture endured at the hands of Israeli interrogators at Al-Jalameh. Loai Ashqar had three of his vertebrae broken due to torture sustained in Al-Jalameh in 2005, permanently paralyzing his left leg. Under Israeli military law, detainees can be held in interrogation for up to 60 days without access to a lawyer, effectively preventing appropriate checks on interrogation methods. [4] G4S commits grave human rights violations across the world: Besides human rights abuses in Israeli prisons, G4S also has a dreadful track record of serious negligence and violent abuse in prisons it runs around the world [4]

## Sources

[1] <https://en.wikipedia.org/wiki/G4S> [2] <https://www.middleeastmonitor.com/20230602-report-private-security-firm-g4s-to-divest-from-israel/> [3] Hever, S. - The privatization of Israeli Security (2018) [4] <https://www.addameer.org/publications/corporate-complicity-israeli-detention-g4s-0> [5] <https://www.ft.com/content/43c2589a-ea4b-11e3-afb3-00144feabdc0> [6] <https://www.whoprofits.org/companies/company/3798?g4s-israel-hashmira>

## IPS Kabarnit Plan

Beginning in 2021, under the IPS Commissioner's leadership and the Technological Division's Head, the IPS started implementing a strategic move designed to lead to a technological leap in the IPS. This strategic move was expressed in the formulation of the multi-year "Kabarnit" plan (the "Kabarnit" Plan), and its implementation began at the beginning of 2022. This plan, according to the IPS, is intended to shape and lead the IPS' new path as a dominant, innovative, and sophisticated security organization, and among other things, to establish an advanced and innovative work environment for the staff while increasing the use of technology, digitization, and innovation. [1]

### Firm

The IPS, the national correctional organization that oversees 30 incarceration facilities, is a security body that holds thousands of criminal and security prisoners in custody. The information about these prisoners, including classified security information and sensitive personal information in the medical, biometric, and intelligence fields, is managed in the organization's information systems. Furthermore, the IPS computers store much information on modus operandi, operations, investigations, and information on the IPS defense and security systems. In addition to the information originating from the organization, the IPS receives classified, operational, and intelligence information from the Police and other agencies. The disclosure of this information to an unauthorized party may result, among other things, in harm to the state, risk human life, the disclosure of information, methods of operation, and covert investigations, and in the foiling of operations. [1]

### Technical Mean

The IPS faces many technological challenges, and to cope with them, it operates through its Technological Division dozens of computerized organizational systems: Operational core systems for prisoner management and intelligence; Medicine and rehabilitation; Personnel, training, and logistics; Diverse security systems installed in incarceration facilities to protect them; Information security and cyber protection systems; And computerized systems in infrastructure, including server farms and a backup site. [1]

### Objectives

Implementation and Integration of Technologies in the Operational Core Systems – in 2022, the Technological Division, as part of the "Kabarnit" multi-year plan,

implemented new technological systems such as digital diaries, a digital prisoner file, and multidimensional monitoring systems as part of the transition to a “smart prison” [1]

## Target

Palestinian Prisoner rights group Addameer has described the Israeli prison system as a “complex of monstrous machinery in form, laws, procedures, and policies...designed to liquidate and kill”. Today, the number of Palestinians currently behind Israeli bars is 5,200, including 33 women and 170 children. If tried, Palestinian prisoners are prosecuted in military courts. ... Since the outbreak of the second Intifada in 2000, more than 12,000 Palestinian children have been detained by Israeli forces.[2]

## Effects

One in every five Palestinians has been arrested and charged under the 1,600 military orders that control every aspect of the lives of Palestinians living under the Israeli military occupation. That incarceration rate doubles for Palestinian men – two in every five have been arrested. [2]

## Sources

[1] Digital Technologies and Information and Cyber Protection in the Israel Prison Service <https://www.mevaker.gov.il/sites/DigitalLibrary/Documents/2023/2023.5-Cyber/EN/2023.5-Cyber-104-Jail-Taktzir-EN.pdf> [2] <https://www.aljazeera.com/news/2023/10/8/why-are-so-many-palestinian-prisoners-in-israeli-jails>



# Intelligence

## Unit 8200

8200 יחידה, Yehida shmone matayim “Unit eight two-hundred”

An Israeli Intelligence Corps unit of the Israel Defense Forces. Composed primarily of 18–21 year olds. The culture of Unit 8200 resembles that of a start-up, according to former officers. Soldiers work in small groups, with limited resources, to crack challenges that – literally, in some cases – are life-and-death matters. Disruptive behaviour and challenges to authority are encouraged, even if this means defying senior officers. [3,5] Also includes Unit 81, which focuses on providing newly invented technology (typically integrated hardware-software products) to combat soldiers [5]

the largest and most central collection unit, responsible for amassing all intelligence transmissions, including phone calls, text messages, and emails. ... soldiers from Unit 8200 use their routine surveillance on Palestinians in the OPT to extort or try them and documenting a wide variety of personal information that can be used to extort Palestinians into serving as informants or otherwise collaborating with the Israeli military and Shin Bet: including financial difficulties, sexual orientation, serious illness, or medical treatments needed by a loved one” [9, p 103]

Firm

Israel fed the best of its brainpower into its elite military intelligence service, known as Unit 8200. ... Innovation mattered above all in Unit 8200, and innovation could come from anywhere in the ranks. ... The young techs might spend their days and nights listening in on suspected terrorist cells, disabling an enemy’s early-warning system before an Israeli airstrike, helping to engineer the Stuxnet malware that crippled Iran’s nuclear program, or providing eyes and ears (by remote) for a secret combat mission.” [7, p188/189]

- \* Former Unit 8200 soldiers have, after completing their military service, gone on to founding and occupying top positions in many international IT companies and in Silicon Valley.[3]
- \* Some of the Google employees associated with Unit 8200 include Gavriel Goidei (Head of Strategy and Operations at Google, previously served as “Head of Learning” at the Unit, where he described working with a team to “understand patterns of hostile activists.”), Jonathan Cohen (Head of Insights at Google), Ben Bariach (Google’s “product partnership manager.”)
- \* Companies such as CheckPoint, Imperva, Nice, Gilat, Waze, Trusteer, and Wix all have their roots in this IDF unit. [2]
- \* Companies with founders who have been through the 8200: Argus Cyber Security

(Ben-Noon, Lavi, Galula), Adallom (Rappaport, Luttwak, Reznik), Palo Alto Networks (Zuk), NSO (Hulio), CyberArk (Mokady), Imperva (Kramer), Check Point Software Technologies (Shwed), Hyperwise Security (Gafni, Omelchenko), FST Biometrics (Frakash), Radware [2]

\* Brigadier General YS. / Yossi Sariel (wrote book “The Human-Machine Team” with the IDF’s permission after a year as a visiting researcher at the US National Defense University in Washington DC and was leading member of a group of academically minded spies known as “the Choir”) [1]

\* a new “advanced technologies park” is rising from the sandy soil of the Negev desert. It aims to cement those links and draw in investors from the wider world who want to benefit from Israel’s cyber expertise. The project combines an office park – whose tenants include Deutsche Telekom, IBM, Oracle, Lockheed Martin, EMC and PayPal – with Beer Sheva’s Ben-Gurion University and its Cyber Security Research Centre. By the end of the decade, Unit 8200 and the IDF’s other intelligence and technology units will have moved there [5]

\* FORBES estimates [that] more than 1,000 companies have been founded by 8200 alumni, from Waze to Check Point to Mirabilis, the parent company of ICQ. Tech giants like to gobble up 8200 firms like hors d’oeuvres. In the last three years alone, Microsoft bought Adallom, a data privacy firm, for a reported \$320 million; Facebook bought mobile analytics company Onavo for some \$150 million; and PayPal grabbed CyActive, which predicts hacks, for an estimated \$60 million. [6]

\* Radinsky (winner of the Israel Defense Prize, part of Unit 81) developed algorithms for Microsoft and cofounded SalesPredict which is staffed by 8200 alums [6]

\* Nadav Zafrir, the 46-year-old CEO and cofounder of Team8, runs a private foundry that creates startups from scratch to solve some of the toughest problems in cybersecurity. He served as 8200’s commander for five years, leaving in 2013 after founding the IDF’s “Cyber Command,” an elite group of geeks that oversees the military’s online warfare. Along with his two cofounders, also high-level 8200 alums, Zafrir raised \$40 million in seed money and an all-star lineup of research partners and investors that includes Alcatel-Lucent, Accenture, AT&T, Cisco, Nokia and Eric Schmidt’s Innovation Endeavors [6]

\* Many retired officers have set up commercial companies in the security, armament, and information technology (IT) areas, creating a continuum between the IDF and commercial, financial, and industrial Israel. The IT industry is owned mainly by such officers. [8]

## Technical Means

\* Developing/operating world-class hacking and artificial intelligence tools as warfare moves from conventional battlefields – land, sea and air – to include cyber terrain. [5]

\* Gospel, Lavender (link to other entries?)

\* <https://en.wikipedia.org/wiki/Duqu>

## Objectives

- \* responsible for clandestine operation, collecting signal intelligence (SIGINT) and code decryption, counterintelligence, cyberwarfare, military intelligence, and surveillance. [3]
- \* similar to that of the NSA or Britain's Government Communications Headquarters, covering everything from analysis of information in the public domain to use of human operators and special signal intelligence. [5]

## Targets

- \* Its geographical remit is primarily outside Israel but it does include the Palestinian territories. [5]
- \* True to its mission, even the recruiting is clandestine [6]

## Effects

- \* Start-up Nation (Dan Senor and Saul Singer, 2009) describes Israel's start-up culture and sees unit 8200 and other elite units as "the nation's equivalent of Harvard, Princeton and Yale". [5]

## Sources

- \* [1] Top Israeli spy chief exposes his true identity in online security lapse](<https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse>)
- \* [2] <https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley>
- \* [3] [https://en.wikipedia.org/wiki/Unit\\_8200](https://en.wikipedia.org/wiki/Unit_8200)
- \* [4] <https://www.projectcensored.org/big-tech-hires-hundreds-of-ex-israeli-spies/>
- \* [5] <https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c>
- \* [6] <https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#58ed1c501a51>
- \* [7] Laurent Richard & Sandrine Rigaud, 2013, Pegasus. The secret technology that Threatens the End of Privacy and Democracy.
- \* [8] An Army Like No Other, How the Israel Defense Forces Made a Nation - Haim Bresheeth-Žabner 2020, H1
- \* [9] Towers of Ivory and Steel: How Israeli Universities Deny Palestinian Freedom - Maya Wind (2024)

## Image, Text, and Facial Recognition

## Homeland Security Text Mining

The use of AI to go through online texts and documents procured by the IDF in physical searches, to decipher the meaning of communication between or about Hamas operatives and their activities.

### Firm

IntuView Ltd, an Israeli based software company in the area of natural language processing.

Founder: Shmuel Bar, a former Israel intelligence official. Advisory board: Shabtai Shavit, Former Head of Mossad and James Woolsey, Former Director of the CIA [3]

### Technical Means

AI used to assess texts to determine whether they contain content deemed of a terrorist nature or of intelligence value. It provides an Intelligence Analysis Report and feeds the results into the user's database for integration with other intelligence data [2]. It is "not a translation but an interpretation service that mines the meaning of texts often hidden in cultural metaphors and religious sayings" [1].

### Objectives

Faster processing of documents to obtain military intelligence: communication between or about Hamas operatives and their activities and the locating of hostages. IntuView promotes its product as a way to avoid human error in the interpretation of documents that require intimate knowledge of the religious, social, organizational and political milieu of the document's creators.

### Target

Locating Hamas operatives and hostages [2].

### Effect

Most likely the effect is misinformation because IntuView's founder Bar admits it isn't a finished system yet: "It will be months before we finish the R&D. In the meanwhile, hundreds of soldiers would have died because the IDF didn't receive the intel it needed," and "We are minimizing the losses even though the system isn't yet perfect." The accuracy rate is currently at 70 percent.[1]

## Sources

- \* [1] [Israel's Military-Technology Complex Is One of a Kind](#) Foreign Policy (19-12-2023).
- \* [2] [DOCEX for Homeland Security](<https://www.intuview.com/homelandsecurity>) IntuView (12-04-2024).
- \* [3] [IntuView: Team](#) IntuView (12-04-2024).

## Corsight

### Firm

Founder Aaron Ashkenazi - ex Shin Bet - Managing partner of Awz ventures, Canadian-Israeli venture capital fund

### Technical Means

- \* Corsight software
- \* Google Photos

“The Israeli military has supplemented Corsight’s technology with Google Photos – which, unlike Corsight, is free to use – soldiers told the Times. Intelligence officers have uploaded databases of “known persons” to Google Photos and used the photo search function to further identify people. One officer told the Times that Google Photos could identify people even when only a small portion of their face was visible, making it better than other tools, including Corsight.”

“Corsight AI is a part Israeli-owned facial recognition company that works with the notoriously brutal police departments in Mexico and Brazil and the Israeli government. A former Israeli army colonel, Dany Tirza, partnered with Corsight AI to develop a police body camera that could immediately identify an individual in crowds, even if their face was covered, and match the person to photographs from years before.” [5, p64]

Table: Promotional claims by Corsight on [their website](#)



	Corsight FORTIFY	Competitors
Min Face Size	Min 40 Pixels ear-to-ear	Min 50 Pixels ear-to-ear
Side Angles	90	+/- 45
Elevation Angles	45	+/- 30
% of Face Required for Recognition	50	70
Dark/Mirrored Sunglasses	Positive Recognition	Recognition Reduced
Full Recognition in Dark	Yes	No
Live/Real-Time Matching Alerts (per1000 faces)	0.01 ms	+ 0.43 ms
Outdated Reference Images	Up to 30 Years	Up to 10 Years

## Objectives

- \* Identify Hamas operatives at checkpoints
- \* Create a "hit list" of people who participated in Oct 7th attacks
- \* Gather more photos for the facial recognition database
- \* Identify victims and casualties in hospitals

## Target

- \* Palestinian population

## Effects

- \*

## Innaccuracies

"In some instances, Corsight's tool mistakenly identified people as being connected to Hamas. One such case involved Palestinian poet Mosab Abu Toha, who was plucked from an Israeli military checkpoint on Gaza's central highway in mid-November while he was trying to leave Gaza for Egypt with his family. The system had flagged Abu Toha as being on an

Israeli list of wanted persons. Israeli officers held Abu Toha in a detention facility, where he was beaten and interrogated for two days before being returned to Gaza without an explanation.”

## Sources

\*

[Israel Deploys Expansive Facial Recognition Program in Gaza](#), The New York Times

\*

[Israel quietly rolled out a mass facial recognition program in the Gaza Strip](#), The Verge

\* [Unity and hi-tech: Israel's tools to recover from Hamas's war - opinion](#) op ed by founder Aaron Ashkenazi

\*

[Google Won't Say Anything About Israel Using Its Photo Software to Create Gaza "Hit List"](#), The Intercept

\*

[5] Antony Loewenstein - The palestine laboratory (2023)

## COGITO4M / COGITO 1003 / SmartForms AI

COGITO4M is an enterprise scale mobile automated interviewing and interrogation system. COGITO 1003 is an automated interviewing and interrogation Kiosk system which allows screening and investigation of many employees, travelers or suspects at crime scene. SmartForms© is an advance AI (Artificial Intelligence) technology which enables accurate questionnaire filling analysis. These algorithms enable detection of false reporting in online forms. The AI SmartForm algorithm is studying of the examinee behavior while filling up the online form compare it to known behavior patterns for tens of thousands of examinees who filled up similar forms before.

Firm

Suspect Detection Systems (SDS) is a leader in counter terrorism and crime prevention behavior pattern recognition technologies. SDS was established by former seniors from security agencies and machine learning experts. The company line of products has an established track record in helping law agencies enforcement and enterprises to mitigate crimes and terrorists activities. SDS invested hundreds of man years and joint efforts of studies with US Department of Home Land Security and security agencies in Israel and many other countries. That huge database and know how become part of SDS technology trough using advance algorithms. Using “Guilty Knowledge” and “Stimulated Reaction” methods and utilizing advance sensors such as P300, GSR, BVP and Thermal Imaging analysis allow SDS to build coherent line of products that revolutionize the war against terrorists and criminals. [2]

Technical Mean

The Cogito SDS includes a suitcase that holds a laptop (with an in-built web camera), headphones, fingerprint recorder and a palm sensor cradle that detects the psychophysiological reaction. The left hand is placed securely in the ergonomic palm sensor which provides the biofeedback. The power panel is located on the bottom right side of the system (Suspect Detection System, 2021). The software components of the system include the in-built software that is responsible for the analysis of the skin conductance and the generation of the results of the test. Questions are presented to an examinee in both audio and visual format in the screen. The Cogito technology is an automated decision making system where in it “does not require any other external device or tool for analysis” (Vaya, et al., 2010, p. 106). It collects and analyses the psychophysiological signal, cross-references these markers with additional objective information and finally identifies and isolates those that it detects as suspects (having malicious intent). Another version of the Cogito SDS is kiosk

based. The kiosk contains two industrial personal computers, a touch screen display, a noise cancellation headset, a microphone, a bar-code reader, a galvanic skin response sensor built into an ergonomic palm case, a video camera, and a seat for the examinee. It has an administration station that is used to monitor the kiosk. [1]

#### Objectives

The technology uses the concept of stimulated psychophysical reaction (SPRR) which is based on stimulating examinees with specific crime-related triggers

#### Sources

[1] <https://ijip.in/wp-content/uploads/2023/01/18.01.168.20221004.pdf> <https://matzav.com/israels-top-10-airport-security-technologies/> [2] <https://www.sds-cogito.com/> [3] <https://www.sds-cogito.com/products-new>

## **“Better Tomorrow” / Google Ayosh / OnWatch / OnAccess / OnPatrol / SesaMe**

The company’s core product is designed to pick out the faces of multiple suspects in a large crowd, monitor crowd density and track and categorize different types of vehicles, according to promotional materials. AnyVision has described this system as “nonvoluntary” because individuals do not need to enroll to be detected automatically. The company claims to have deployed its technology across more than 115,000 cameras. [7]

### Firm

- \* AnyVision, now called Oosto. “AnyVision is an Israeli start-up that secretly monitors Palestinians across the West Bank with a range of cameras, the location of which are not acknowledged by the company or Israel. Artificial Intelligence thus merges with biometrics and facial recognition at dozens of Israeli checkpoints throughout the West Bank. [5, p63]
- \* Carnegie Mellon University’s (CMU) CyLab Biometric Research Center (collaboration will help Oosto address a broad range of safety-related use cases, including object detection (e.g., weapons on school grounds) and behavioral analysis (e.g., when someone falls down)) [2]
- \* In March 2020 Microsoft divested its USD 74 million stake in AnyVision after protests by its employees and an audit led by former US Attorney General Eric Holder which concluded that ‘the technology is used at border crossing checkpoints between Israel and the West Bank’, whilst noting that ‘available evidence demonstrated that AnyVision’s technology has not previously and does not currently power a mass surveillance program in the West Bank that has been alleged in media reports.’ Several former AnyVision employees, who did not want to be named because they had signed nondisclosure agreements and feared retaliation, told NBC News that the company did not adhere to Microsoft’s ethical standards. [7]

### Technical Mean

- \* An ‘advanced tactical surveillance’ system called Better Tomorrow is being used by the Israelis across the West Bank and East Jerusalem to monitor the movement of Palestinians and deter attacks. [3]
- \* “.. digging by NBC News uncovered a project, called Google Ayosh, targeting all Palestinian with the use of big data. AnyVision continues to use the occupation as a vital source to train its systems in the mass surveillance of Palestinians, focusing, it says, on attempts to stop any Palestinian attackers” [5, p63]
- \* AnyVision boasts the ability to remotely and covertly install its software on any camera,

even those that are relatively low-tech. If marketing materials are to be believed, “Better Tomorrow”, the software system purportedly used in the West Bank, can trace a person-of-interest across multiple cameras; find repeated appearances of an individual; detect suspects and suspicious objects caught on camera; rapidly perform historic video analysis for forensic purposes; and extract, analyze and store face images of all individuals who pass within a camera’s view. [6]

\* Palestinian teenagers outside Ramallah had discovered a hidden surveillance system and video camera purportedly made by AnyVision camouflaged in a false rock in a cemetery [6] AnyVision has a product, called SesaMe, that offers identity verification for banking and smartphone applications. [7]

## Objectives

\* “Rapid and accurate real-time, real-world face, body, and human behavior video analytics.” [1]

\* At newly upgraded checkpoints, Palestinian workers with permissions to work in Israel, who have been granted biometric IDs, simply approach an optical turnstile, scan their digital IDs, and stare into a camera. Within seconds, AnyVision’s facial recognition software is able to authenticate their identity. If verified, electronic panels open [6]

\* “Israeli officials, and many Palestinian day laborers, praise the new checkpoint system for its efficiency. Dubbed “Speed Gate,” it “allows the Palestinian population to cross in very short time spans,” [4]

## Target

\* The facial recognition software used to identify Palestinians at checkpoints was developed by the Israeli tech company AnyVision [4]

\* AnyVision’s technology is being deployed throughout the West Bank in a separate, “much more confidential” program to track “potential Palestinian assailants.” [4]

## Sources

\* [1] <https://oosto.com/>

\* [2] <https://oosto.com/press/anyvision-now-oosto/>

\* [3] <https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/anyvision-google-ayosh-palestinian-surveillance>

\* [4] <https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc>

\* [5] Antony Loewenstein - The palestine laboratory (2023)

\* [6] BIOMETRICS AND COUNTER-TERRORISM Case study of Israel/Palestine (2021) -

<https://privacyinternational.org/sites/default/files/2021-06/>

PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel\_Palestine%20v7.pdf

\* [7] [Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?](#) NBC

Oct. 28, 2019

## Blue Wolf

smartphone technology called Blue Wolf that captures photos of Palestinians' faces and matches them to a database of images so extensive that one former soldier described it as the army's secret "Facebook for Palestinians." The phone app flashes in different colors to alert soldiers if a person is to be detained, arrested or left alone. the surveillance of Palestinians has become gamified. For example, two soldiers stationed in Hebron in 2020 said another system - known as Blue Wolf, operated through an app - generating rankings based on the number of Palestinians registered, with Israeli commanders giving prizes to the battalion with the highest score. In this way, Israeli soldiers are incentivised to keep Palestinians under constant observation. [3]

## Wolf Pack

One of them told The Post that this database is a pared-down version of another, vast database, called Wolf Pack, which contains profiles of virtually every Palestinian in the West Bank, including photographs of the individuals, their family histories, education and a security rating for each person. This recent soldier was personally familiar with Wolf Pack, which is accessible only on desktop computers in more secure environments. (While this former soldier described the database as "Facebook for Palestinians," it is not connected to Facebook.)

## White Wolf

A separate smartphone app, called White Wolf, has been developed for use by Jewish settlers in the West Bank, a former soldier told Breaking the Silence. Although settlers are not allowed to detain people, security volunteers can use White Wolf to scan a Palestinian's identification card before that person enters a settlement, for example, to work in construction. military in 2019 acknowledged existence of White Wolf in a right-wing Israeli publication.

## Hebron Smart City

A wider network of closed-circuit television cameras, dubbed "Hebron Smart City," provides real-time monitoring of the city's population and, one former soldier said, can sometimes see into private homes.

The photos taken by each unit would number in the hundreds each week, with one former soldier saying the unit was expected to take at least 1,500. Army units across



the West Bank would compete for prizes, such as a night off, given to those who took the most photographs, former soldiers said.

Israeli occupation takes a heavy toll on our physical and psychological wellbeing, and knowing that we are constantly under surveillance adds to our suffering. We not only have to deal with constant harassment by Israeli soldiers, stop and search abuses, arbitrary arrests and extrajudicial killings, but we also do not feel safe in our own homes, when we are surfing the web, talking on the phone, conversing with our friends.

[2]

## Sources

\* [Israel escalates surveillance of Palestinians with facial recognition program in West Bank](#)

Washington Post, November 8, 2021

\* [2] Under Israeli surveillance: Living in dystopia, in Palestine [https://](https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine)

[www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine](https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine)

\* [3] <https://www.amnesty.org.uk/press-releases/israel-using-previously-unreported-facial-recognition-system-automate-apartheid>

## Red Wolf

The Israeli authorities are using a previously-unreported experimental facial recognition system known as Red Wolf to track Palestinians and automate harsh restrictions on their freedom of movement [2]

## Firm

high-resolution CCTV cameras made by the Chinese company Hikvision installed in residential areas and mounted to military infrastructure; some of these models, according to Hikvision's own marketing, can plug into external facial recognition software. Amnesty International also identified cameras made by a Dutch company called TKH Security, in public spaces and attached to police. infrastructure. [1]

## Technical Mean

"There's something like ten cameras [inside the checkpoint]. Once they arrive and pass through inside, it essentially takes photos, identifies them, to help you as the soldier standing there. It catches the face before [they enter], and it displays the face for you on the computer. If it's someone who's been coming through there a lot, the computer already knows them. It takes photos of everyone who passes there

essentially. And you, as a soldier, a commander, standing there, can match the face to the IDs until the system learns [to recognize] the face. It recognizes him, and then he comes, and he's already lit green for me even before he showed me an ID, and so it makes the process shorter for him, in theory." [3] When a Palestinian goes through a checkpoint at which Red Wolf is operating, their face is scanned without their knowledge or consent and compared with biometric entries in databases which exclusively contain information about Palestinians. Red Wolf uses this data to determine whether an individual can pass a checkpoint and automatically biometrically enrolls any new face it scans. If no entry exists for an individual, they will be denied passage. Red Wolf could also deny entry based on other information stored on Palestinian profiles, for example if an individual is wanted for questioning or arrest. [2] Amnesty also documented how Israel's AI-powered facial recognition systems are supported by a vast physical infrastructure of surveillance hardware. [2]

## Objectives

Similarly, to Blue Wolf, using the system is gamified as well: "The battalion had a competition who put in the most new names. It's a system where, ultimately, you, as a person at the checkpoint, teach it. It takes photos. I can go into the photo after and then put in the ID". [3]

## Target

The information that is pulled is used to subsequently decide whether an individual may or may not pass a checkpoint. 175 Palestinians are the only racial group of residents in H2 required to use these checkpoints, 176 and the system relies on databases consisting exclusively of Palestinian individuals' data. Jewish Israeli settlers use different roads and are not required to cross such checkpoints. [3]

## Effects

Eyad also described how Israeli soldiers seem to rely on the facial recognition system, which Amnesty International identified as Red Wolf, to bar residents from returning to their homes: "They [Israeli soldiers] can tell you that your name is not in the database, as simple as that, and then you're not allowed to pass through [to] your house." [1]

## Sources

[1] <https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/> [2] <https://>

[www.amnesty.org.uk/press-releases/israel-using-previously-unreported-facial-recognition-system-automate-apartheid](https://www.amnesty.org.uk/press-releases/israel-using-previously-unreported-facial-recognition-system-automate-apartheid) [3] AUTOMATED APARTHEID (2023) -  
[https://www.amnesty.org.uk/files/2023-05/Automated%20Apartheid.pdf?  
VersionId=hKRPW/bz18UpH1w1kyx9RgbJoChyWKWxU](https://www.amnesty.org.uk/files/2023-05/Automated%20Apartheid.pdf?VersionId=hKRPW/bz18UpH1w1kyx9RgbJoChyWKWxU)

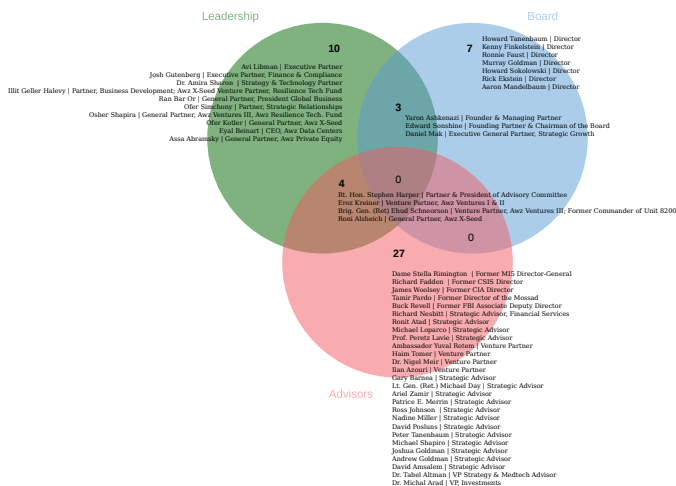
## Venture Capital

# AWZ Ventures

Venture capital fund <https://www.awzventures.com/about>

## Firm

Awz is in an unparalleled position to identify, evaluate and invest in multi-purpose, defensive technologies with the greatest commercial potential thanks to: Our unique partnership with MAFAT (the Israeli Ministry of Defense's Directorate of Defense R&D) and its partner agencies



## AWZ Ventures Leadership

## Portfolio

[https://codeberg.org/IDS/t4g\\_map/src/branch/main/data/awz-portfolio-data.csv](https://codeberg.org/IDS/t4g_map/src/branch/main/data/awz-portfolio-data.csv)

## Team & Board of directors

<https://www.awzventures.com/our-team>

## How to contribute

Select some articles in the reading list to identify entities, systems, products, etc...

Fill this template and copy/paste it in the appropriate section

### Title

#### Firm

#### Technical Mean

#### Objectives

#### Target

#### Effects

#### Sources

## Reading list (to do)

TIP online presentations: Palestine for Tech workers - Digital Walls (A four-part info session for tech workers and activists who don't want to be complicit in – and instead contribute to ending – Israeli oppression of the Palestinian people) <https://www.youtube.com/playlist?list=PLv7n0tLce-KIYf-U11sUyovfeE1P473Bp>

maybe examples can be extracted from the reading below.

\*

[Israeli startups hope to export battle-tested AI military tech](#), Nikkei Asia, March 30, 2024

\*

[Surveillance as a Service: The Global Impact of Israeli “Defense” Technologies on Privacy and Human Rights](#) - Tor project blog, 8 April 2024

\*

[How Israel automated occupation in Hebron | The Listening Post](#) Al Jazeera English

\*

'A mass assassination factory': Inside Israel's calculated bombing of Gaza [+972 Magazine](#)  
Yuval Abraham - November 30, 2023

\*

Documents Reveal Advanced AI Tools Google Is Selling to Israel [The Intercept](#) Sam Biddle - July 24 2022

\*

<https://time.com/6966102/google-contract-israel-defense-ministry-gaza-war/>

\*

Between the Sea and the Security Fence <https://illwill.com/the-sea-and-the-security-fence>

\*

Israeli Group Claims It's Working With Big Tech Insiders to Censor “Inflammatory”

## Wartime Content

<https://theintercept.com/2024/01/10/israel-disinformation-social-media-iron-truth/> Ian Alan Paul - October 18th, 2023

\*

The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World [Verso Books](#) Antony Loewenstein podcast: <https://antonyloewenstein.com/verso-podcast/>

\*

The IDF's tech bragging page: <https://www.idf.il/en/mini-sites/technology-and-innovation/the-idf-s-top-10-innovations/>

\*

Inside the Pro-Israel Information War - <https://jackpoulson.substack.com/p/inside-the-pro-israel-information>

\*

<https://www.mei.edu/publications/nowhere-hide-impact-israels-digital-surveillance-regime-palestinians>

\*

<https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/>

\*

<https://www.dair-institute.org/no-tech-for-apartheid-event/> [https://en.wikipedia.org/wiki/List\\_of\\_multinationals\\_with\\_research\\_and\\_development\\_centres\\_in\\_Israel](https://en.wikipedia.org/wiki/List_of_multinationals_with_research_and_development_centres_in_Israel)

\*

<https://www.tni.org/en/article/seeing-the-world-like-a-palestinian>

\*

<https://www.calcalistech.com/ctechnews/article/ydrvduy6z>

\*

<https://www.projectcensored.org/big-tech-hires-hundreds-of-ex-israeli-spies/>

\*



<https://www.truthdig.com/articles/the-big-tech-behind-israels-digital-apartheid/>

\*

<https://mondoweiss.net/2021/12/how-google-advances-the-zionist-colonization-of-palestine/>

\*

<https://mondoweiss.net/2021/03/how-microsoft-is-invested-in-israeli-settler-colonialism/>

\*

<https://www.timesofisrael.com/google-creates-4-million-fund-to-provide-lifeline-to-israeli-ai-startups-during-war/>

\*

<https://ainowinstitute.org/publication/the-algorithmically-accelerated-killing-machine>

\*

<https://watson.brown.edu/costsofwar/papers/2024/SiliconValley>

\*

\*

MIT projects funded by Israeli DoD

\*

<https://mitsage.my.canva.site/>

\*

from there this spreadsheet is linked: <https://docs.google.com/spreadsheets/d/1Q13sdsOQsxTtkqG-lebja5l-6-Oy8ERVhF1-JjOe8G8/edit#gid=0>

James Bamford on FISA & How U.S. Intel and Palantir Feed Israel's Killing Machine in Gaza [Democracy Now!](#)

- found via: [https://twitter.com/Resist\\_05/status/1786898898512167162](https://twitter.com/Resist_05/status/1786898898512167162)

- NSA giving data to unit 8200 (convo James Bamford + Ed Snowden)

- Palantir part of this

\*

Something on bluewashing? <https://www.haaretz.com/life/television/2022-05-15/ty-article-magazine/.premium/new-israeli-cop-series-shows-you-a-jerusalem-youve-seen-many-times-before/00000180-d631-d452-a1fa-d7ff5cf50000> <https://en.wikipedia.org/wiki/Fauda>

\*

[Xtend raises \\$40m after drone success in Gaza](#)

\*

[IBM: A Major Facilitator of Israel's Surveillance and Security Apparatus](#)

\*

[Who Profits Research Center](#)

<https://twitter.com/GenocideVC>

<https://www.theguardian.com/technology/article/2024/may/17/ai-weapons-palantir-war-technology> <https://www.bbc.com/news/articles/cger582weplo> Microsoft suspending accounts of ppl calling to Gaza