Episode Book

EPISODE #5952

Inside Malmab: Israel's Most Secretive Security Body

PUBLISHED	14 October 2026 at 09:17 UTC
DURATION	25:58
LISTEN	myweirdprompts.com/episode/malmab-israel-defense-security-96233/
HOSTS	Corn, Herman, Hilbert
SCRIPT MODEL	deepseek-flash
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.4
SOURCES	12 cited by the research (listed at the end)
BOOK GENERATED	19 October 2026 at 17:41 UTC

SYNOPSIS

Most people know Mossad, Shin Bet, and Aman — but there's a fourth body inside Israel's Defense Ministry that almost no one can name. Malmab, the Director of Security of the Defense Establishment, protects the country's most sensitive nuclear and biological facilities, and its practices reveal how governments actually organize information security when a breach could be catastrophic. From clearances that expire in practice to compartments that can't be acknowledged, this episode explores the gap between cybersecurity and true information security — and asks which of these extreme measures could ever make sense for an ordinary business.

TRANSCRIPT



Corn

There's a photograph from the ceremony in Tel Aviv. Netanyahu there, Katz there, the outgoing chief, the incoming one. Everything about it says state occasion. Nothing about it tells you what the body being handed over actually does.



Herman

And most Israelis, if you stopped them on the street, could not tell you the name of it.



Corn

Daniel sent this one in. He starts from the three names everybody knows, Mossad, Shin Bet, Aman, and then points out there's a fourth, less familiar body inside the Defense Ministry with specialized security responsibility. Malmab. The Director of Security of the Defense Establishment.



Corn

His actual question isn't really about the org chart. He's using Malmab as a door into something bigger. How do governments, intelligence agencies, defense contractors and nuclear facilities organize information security when a breach could be catastrophic? What do they do that a normal company doesn't? And which of those practices could ever make sense for an ordinary business, and which are so expensive and restrictive they only make sense when the secret is national-security grade.



Herman

He's also poking at a distinction I think is the real spine of this. Most of us equate information security with cybersecurity. Firewalls, endpoint detection, the stuff you buy. In these environments it's much wider than that. It's who is allowed to know what, and how you keep that boundary from eroding through totally mundane operational processes.



Corn

So let's start with the body that got Daniel curious in the first place.



Herman

Malmab was founded in 1958. First director, Haim Kermun, a former Shin Bet officer. It sits inside the Ministry of Defense and its jurisdiction covers the institutions that develop and produce weapons of mass destruction and the defenses against them. The Shimon Peres Negev Nuclear Research Center, the Israel Institute for Biological Research, Soreq.



Corn

So the things you don't read about.



Herman

The things you don't read about. And the remit is wider than protecting a building. Security vetting and audits. Certification of exposure technology. Corruption inquiries. Preventing leaks of classified information. And, this is the part I find surprising, running agents abroad to obtain technological intelligence.



Corn

Run that past me again.



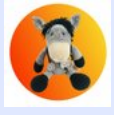
Herman

That role was transferred to Malmab in 1986 after the Pollard affair, from an office called Lekem, the Science Affairs Bureau. So this is not just a guard service. It inherited a collection capability.



Corn

So the security office had a second job dropped into its lap because a different office blew up.



Herman

Effectively. And here's what makes it interesting for our purposes. For all that reach, its budget and its activities are absent from the ministry's annual Freedom of Information report. The ministry website mentions it exists. That's roughly where the public record



Herman (continued)

stops.



Corn

The department that hides its own numbers.



Herman

Which tells you something about how the institution thinks about disclosure, and we're going to come back to that, because the same instinct has been applied to things that had nothing to do with weapons.



Corn

Before we get there, let me try to lay out the general architecture, because Daniel's question is really about the model, not the Israeli instance of it. And the cleanest place to see the model is the American paperwork, because they publish it.



Herman

They do, and the first thing the American system does is separate two things everybody else conflates. Clearance and access are different.



Corn

Which sounds like a small distinction and is actually the whole thing.



Herman

You can hold a favorably adjudicated Top Secret clearance and still not be allowed in the room. For Sensitive Compartmented Information, SCI, you need the clearance, then you need SCI access approval, then indoctrination into the specific program, and often a polygraph. The clearance says the government has decided you're trustworthy. It says nothing about whether you need to know this particular thing.



Corn

So trust is the entry ticket and relevance is the door.



Herman

And the relevance test has a name. Need-to-know. There's a formal definition in the old DCID 1/19. It's a determination by an authorized holder of the information that a recipient requires it for a lawful function. Not a vibe. A documented decision by a named person.



Corn

The word that keeps landing for me is 'holder.' Somebody holds the information and somebody has to sign that this other person requires it. You can't just have the clearance and wander.



Herman

Right, and that's where it gets operationally interesting, because need-to-know is enforced through physical space as much as through rules. The SCIF. Sensitive Compartmented Information Facility. An accredited room where SCI can be processed, stored, used or discussed.



Corn

Accredited by whom?



Herman

By the agency's own accrediting authority, against a standard, ICD 705. Uniform physical and technical security. And TEMPEST countermeasures, which is the fun one. TEMPEST is about electronic emanations. The idea that a screen or a cable radiates enough of a signal that somebody in a van outside can reconstruct what's on it. So you build the room to contain the emanations.



Corn

Somebody in a van reconstructing your monitor from the reflections off the window.



Herman

That's not a joke, that's the threat model. And there's a reciprocal-use rule across agencies, so an accredited facility can be used by another agency under agreed conditions. Which matters enormously in practice, because the alternative is building your own SCIF in every city.



Corn

Cost of paranoia, item one.



Herman

Item one. And then you go up a level, and this is the layer I think Daniel is really asking about, which is program-level compartmentation. In the intelligence community these are called Controlled Access Programs, CAPs. They protect what the directive calls the nation's most sensitive and critical intelligence sources, methods and activities.



Corn

And some of them are unacknowledged.



Herman

Which is a hell of a concept. Unacknowledged means the existence of the program is itself classified. There's no line item, no office, no name. Access runs on two mechanisms. A billet list, which is a fixed number of slots, like seats at a table. And a bigot list, which is by name. Both require approval at the top, and both get revalidated annually. The point is that the population of people who know is a number somebody maintains.



Corn

So the countable thing is the people.



Herman

And the population is deliberately kept small, which is the design, and which is also the cost, and we'll come back to that, because a tightly compartmented organization is slow.



Corn

Slow how? Give me the concrete version.



Herman

Say you need a piece of analysis from a team that isn't read into your program. In a normal office you walk over and ask. In a compartmented environment you can't do that. You either get that person read in, which takes weeks and a signature from someone senior, or you rewrite the request so it doesn't reveal what you're working on, which takes almost as long and produces worse work. So the friction is real and it's daily.



Corn

And that friction is the price of the small population.



Herman

It's the same trade in both directions. You shrink the circle to reduce the chance of a leak, and shrinking the circle reduces the chance that the right people can help each other.



Corn

What about the ongoing monitoring? Everybody I know in a normal job clears a background check once and then it's done forever.



Herman

That's the paradigm shift. The old model was periodic reinvestigation, every five years or whatever the cycle was. The current standard says continuous personnel security and counterintelligence evaluation will be required of all personnel granted access to SCI. Ongoing. Not a snapshot every five years. A stream.



Corn

What is it actually watching?



Herman

Travel, foreign contacts, financial stress, arrests, changes in behavior reported by coworkers. The doctrine assumes a person's risk profile moves over time and that a five-year gap is long enough for it to move a lot.



Corn

So the clearance is not a certificate you own. It's a status that has to keep being true.



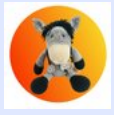
Herman

That's the cleanest way to say it, and I'm going to steal it later in the episode when we get to what transfers.



Corn

Okay. Israel. The contrast.



Herman

The first contrast is bureaucratic. Security clearance in Israel, Sivug Bitchoni, is not adjudicated by Malmab. It's Shin Bet, under the Shin Bet Law of 2002. Levels one through six. Form 3001 questionnaires, personal interviews, polygraph, and an appeals route through an objections committee.



Corn

So vetting the person and protecting the installation are two different organizations.



Herman

Two different organizations, which is a meaningful separation of function. And then the interesting part is where Malmab's actual authority comes from. Under Government Resolution 3611 from August 2011, which set up the civil cyber domain, there's a list of special entities excluded from it. The IDF, Israel Police, Shin Bet, Mossad, and the defense establishment through Malmab.



Corn

Excluded meaning they don't play in the civilian cyber framework.



Herman

They have their own. And Malmab's jurisdiction is defined by reference to the Regulation of Security in Public Bodies Law from 1998, plus suppliers and enterprises developing or manufacturing defense equipment for them.



Corn

So private companies fall inside it.



Herman

They do. And here's the gap the State Comptroller flagged in November 2024. The 1998 law did not clearly confer operational or technological authority on Malmab. It didn't empower it to give professional guidance on specific networks. So you have a body with sweeping practical reach and a statutory basis that doesn't obviously cover what it's doing.



Corn

The body the industry paper said should not exist in a democratic state without legal regulation.



Herman

Israel Defense, 2021, on the appointment of Yuval Shimoni as director. That's the line.



Corn

And you said a new director came in this June.



Herman

Gil Reich, installed at the beginning of June, replacing Shimoni after five years. Cabinet approved him in March. So the body Daniel is asking about has a brand new chief and the same unresolved legal question.



Corn

Let's do Rafael, because it's the concrete case.



Herman

Rafael is one of Israel's top-tier defense firms. The Comptroller's audit found its Technology Security and Cyber Defense Department consumed ten percent of the IT administration's computing budget.



Corn

Ten percent of compute, spent on defending.



Herman

And the more interesting finding is the insurance decision. Rafael declined cyber-incident insurance. Four reasons. Its protection level was considered high enough that the insurance was economically inefficient. Classified information cannot be disclosed to insurers, which kills the whole claims process. And the coverage available capped around ten million dollars, which for a firm of that size is immaterial. It's not worth the paperwork.



Corn

So the risk was small enough they could self-insure, and the policy was useless anyway because you can't describe the incident.



Herman

That second reason is the one I'd put on a slide. The insurance product requires disclosure. The security requirement forbids it. So the product cannot exist for this customer.



Corn

And the same audit found doctrine gaps even there, right?



Herman

It found Rafael failed to disclose several cyber incidents to its board, failed to investigate incidents from 2020 to 2022, and had inconsistent penetration-testing frequency. So this is not a story about a firm doing everything perfectly. It's a story about a firm with an enormous security budget and uneven discipline.



Corn

The budget is the easy part. The discipline is the hard part.



Herman

Which is the through-line of the entire episode. The controls that matter are the ones that depend on a person remembering to do something boring.



Corn

When we did the episode on how need-to-know migrates from state secrecy into Zero Trust architecture, we ended up in roughly this place, that the technical controls scale and the human ones don't.



Herman

They don't, and Zero Trust doesn't have an answer for it. Zero Trust is a network posture. It has no opinion on whether a cleared engineer told his brother-in-law what he saw at work.



Corn

Which is the insider problem, and it's the oldest one.



Herman

The intelligence community treats insider risk as a personnel problem first. That's the doctrine. Continuous evaluation, need-to-know discipline, the by-name list. The technology is the backstop.



Corn

And there's a version of this that ordinary companies are already adopting without knowing it. Least privilege is need-to-know with a different accent.



Herman

It is. Role-based access control is a billet list by another name. The difference is that a big company grants access because a manager clicked approve, and the intelligence community grants it because a named authority documented that the recipient requires the information for a lawful function and reviews the population every year.



Corn

The annual revalidation is the part nobody does.



Herman

Nobody does, and it's the cheapest of all of these. You don't need a SCIF to ask once a year whether each person still needs each access. That's a spreadsheet.



Corn

Item one on the transferable list.



Herman

The second is continuous evaluation, which in a corporate setting is much less invasive than it sounds. It's not polygraphs. It's monitoring for the things that are already in your HR system, plus flagging unusual data access patterns. The intelligence version is heavier because the stakes are higher, but the shape is the same.



Corn

What about the polygraph?



Herman

That's the dividing line. The polygraph is expensive, it's contested, it's a massive intrusion, and it only pays for itself when a single leak is a catastrophe. You can't put a call center through it.



Corn

And it doesn't even work reliably.



Herman

It doesn't, which is the part that makes it interesting as a case study. The polygraph's real function in these settings is less detection than deterrence. People behave differently when they think they'll be asked about it. So you're buying a psychological effect, not a measurement.



Corn

That's a very expensive way to buy a psychological effect.



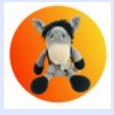
Herman

It is, and that's exactly why it doesn't transfer.



Corn

The SCIF is the other one.



Herman

The SCIF is a room that costs more than most companies' entire security program, and it exists to stop a van outside from reading a monitor. Unless you have a genuine state-level adversary, that threat doesn't apply to you.



Corn

And the unacknowledged program, that's not transferable at all.



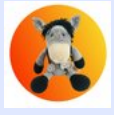
Herman

It's the opposite of transferable. A company that hides the existence of a program from its own board is a company that will be in a courtroom.



Corn

That's the sharp edge. The last time you were mid-story about an audit you'd read, go on.



Herman

I was going to say the top of the range and the bottom of the range use the same three ideas, and everything in between is calibration. Need-to-know, least privilege, revalidation on a schedule. The rest is how much you want to spend on the threat model.



Corn

Alright. So that's the architecture on paper. Now let's look at what happens when the same authority that protects secrets gets turned on the historical record.



Herman

This is the part where the episode stops being an infosec lecture.



Corn

Go.



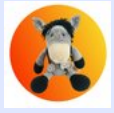
Herman

Starting in the early 2000s, under Yehiel Horev, who ran Malmab from 1986 to 2007, Malmab teams went through Israeli archives and removed historical documents. Not just restricted them. Removed. Including material that had already been declassified and had already been cited by historians.



Corn

Cited in published work.



Herman

Published work. Israel's National Archivist wrote in a 2016 letter that a hundred percent of the examined documentation that remained undisclosed had been concealed with no authority. That's the archivist of the state saying the removals had no legal basis.



Corn

So the same organization that keeps the nuclear research center sealed also decided which documents about 1948 stayed in the file.



Herman

And Horev acknowledged launching the project. His argument was that concealment makes sense because uncovering events from 1948 could generate unrest, and he added that removing documents that had already been published undermines the credibility of studies.



Corn

Read that back.



Herman

Removing already-published documents undermines the credibility of the studies built on them.



Corn

So the objective is to make the record unverifiable.



Herman

That's what the sentence says. And then there's the ratchet, which is the structural part. Confidentiality on the Shin Bet and Mossad archives was set to expire after fifty years back in 1998. It moved to seventy years in 2010. In February 2019 it moved to ninety.



Corn

Fifty to seventy to ninety.



Herman

Ninety years means the material is sealed well past the life of anyone who was there. Tuvia Friling is the former Chief Archivist who resigned over this, and his line is the one I keep coming back to. The storage and archival system is not an arm of the state's public relations. The state may impose confidentiality on some of its documentation. The question is whether the issue of security doesn't act as a kind of cover.



Corn

And he adds that in many cases it's already become a joke.



Herman

Yes.



Corn

The horse.



Herman

Horev's own line. If someone writes that the horse is black, if the horse isn't outside the barn, you can't prove that it's really black.



Corn

He says that as a justification. As an explanation of why removing the documents works. The record isn't falsified, it's just absent, and absence is untestable.



Herman

It's a remarkably honest sentence about method.



Corn

Herman, hold on. I want to sit with the shape of it for a second, because that's not a security doctrine. That's a doctrine about what a public record is for. He's saying the archive's job is to not embarrass the state, and the security classification is the instrument.



Herman

And that's the dual-use problem, which I think is the real story here and the thing that separates this from a normal infosec discussion. The same body is doing two jobs with one set of tools. One of them is legitimate and necessary. The other is nothing to do with security at all.



Corn

Which is not an Israeli specialty. Every government with a classification system has used it to bury something embarrassing. The classification system is a great place to hide a decision you don't want to defend.



Herman

Right, and this is where the international comparison gets uncomfortable, because everyone wants the answer to be that one country does it properly and another doesn't. The reality is that the US codifies its compartmentation powers in executive orders and intelligence community directives, and the Israeli arrangement has the reach without the codification, and both of those can be abused, just through different mechanisms.



Corn

Codification at least gives you a court to go to.



Herman

It gives you a target for litigation. That's a real difference. It means the rule is written down and can be pointed at when it's broken. In the Israeli case the Comptroller had to note that the authority itself is unclear, which makes challenging a specific use of it much harder.



Corn

What about the UK? Is there a comparable framework?



Herman

I don't know on this one, honestly. There's the Developed Vetting and Security Check framework, but I could not find a current government source while pulling this together, so I'm not going to state it as fact.



Corn

Then we flag it as unverified and move on.



Herman

Flagged.



Corn

So Daniel's last question is the one I actually want to get to. What transfers?



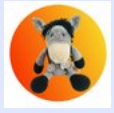
Herman

Three things, and they're unglamorous. Continuous evaluation of access, meaning you keep asking whether the status is still true. Need-to-know discipline, meaning access is granted on a reason and a reason expires. And treating insider risk as a personnel problem rather than a firewall problem, because no firewall has ever stopped someone who was supposed to be in the room.



Corn

And what doesn't.



Herman

Polygraphs. SCIFs. Unacknowledged programs. Ninety-year archive seals. Every one of those buys something real and costs more than a normal organization can pay, and in the case of the archive seals, it costs something that isn't measured in money at all.



Corn

That's where the episode actually lands for me. Compartmentation isn't free. You buy security with collaboration, with speed, and sometimes with the ability of your own public to know what you did.



Herman

And the Rafael audit is the proof that even at the top, with ten percent of the compute budget spent on defending, the doctrine can still have holes in it.



Corn

The controls are only as good as the person doing the boring part.



Hilbert

The horse is a good line. The problem is the barn.



Hilbert

The barn isn't a barn. It's a filing cabinet in a basement in Tel Aviv that was moved twice. I know because I was on a committee that reviewed something adjacent to this, and I want to be clear that I am not claiming anything about what was in it.



Herman

What was the committee?



Hilbert

It was a committee. It was constituted, it met, it produced findings, and I was one of the people who read the findings. It met in a converted falafel stand on Yehuda Halevi. The fryer was gone but the hood was still on the wall, and the chair of the committee used to hang his coat on the hood, which meant the coat smelled of oil, and he complained about it at every session, and we never moved the coat.



Corn

And the filing cabinet?



Hilbert

The cabinet is separate from the committee. The cabinet is the part I actually know about. When Lekem's technological intelligence function was folded into Malmab in 1986, some of the paper moved, and some of the paper stayed where it was, and the reason it stayed is that the man in charge of moving it injured his back carrying the first load and never came back to finish.



Herman

How long?



Hilbert

Four years. The paper sat there for four years, and when it was finally consolidated, three folders were missing, and there are two theories about what happened to them, and I have heard both, and the more popular one is wrong.



Corn

Which one do you believe?



Hilbert

I believe the one about the photocopy.



Herman

The photocopy.



Hilbert

It's not a philosophy. Somebody made a copy. That's what people do. If you have a document you have to hand over and you don't want to hand it over, you photocopy it first. The question is not whether copies exist. The question is where they are now, and the answer is a safe in a flat in Netanya that I no longer have the key to.



Corn

Do you have the photocopy?



Hilbert

I have the safe. I don't have the key. And the flat was never mine. I was housesitting for a cousin.



Herman

Which cousin?



Hilbert

The one who emigrated. I asked him about it and he has no memory of the safe. He has a memory of everything else in that flat. He remembers a lamp. He does not remember a safe.



Corn

A cousin with a perfect memory of a lamp and no memory of a safe.



Hilbert

I've stopped asking. There's no leverage in it. Either the safe opened at some point and I don't know, or it never opened, and either way I'm not getting the folders in this lifetime.



Herman

And you say the folders, plural.



Hilbert

Three. I said three. The popular theory is that they went out with the trash in 1990 and the reason that theory is popular is that it's the one that requires nobody to have done anything wrong.



Corn

And the other theory requires the opposite.



Hilbert

The other theory requires a man to have made a copy and locked it in a safe, which is not a crime, it's just a filing habit, and it is much harder to be angry at.



Herman

It is much harder to be angry at.



Hilbert

That's what I've found.



Corn

I think the thing I'm taking from that is not the folders.



Herman

No.



Corn

It's that the security never had anything to do with the paper. It had to do with the man's back.



Herman

A back injury, a hood, a coat, and four years.



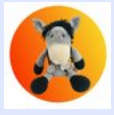
Hilbert

It's usually a back.



Corn

Alright. The open question I want to leave with is this. If the same authority that protects a nuclear research center can also seal a historian's file, then what does that tell you about security as an organizing principle for an institution?



Herman

It tells me the boundary of the authority is the entire business, and that the boundary is almost never written where it needs to be written.



Corn

The ordinary company adopting continuous evaluation and least privilege is inheriting a smaller version of the same tension. You're always deciding who gets to know, and that decision always has a cost, and somebody always eats it.



Herman

The horse isn't outside the barn, and you can't prove it's black.



Corn

If you want more of this, try episode thirty-five, The Privacy Gap; episode five thirty-seven, From State Secrets to Zero Trust; and episode fourteen oh eight, Israel Wartime Readiness Field Guide. This has been My Weird Prompts. Herman Poppleberry produced by Hilbert Flumingtop, who is still at the desk, presumably with a photocopy.



Herman

Presumably.



Corn

If you enjoy the show, leave us a review wherever you listen. It helps. And send us your own prompt on Telegram at t dot me slash MWP listener bot. We'll be back soon.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Israel Ministry of Defense (mod.gov.il) [primary]**
   Gil Reich appointment ceremony, 2026-06-02
   https://mod.gov.il/.../-------

2. **Israel State Comptroller [primary]**
   Cyber Security... at Rafael Advanced Defense Systems Ltd., Nov 2024
   https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2024/2024.11-Cyber/EN/Cyber-106-Refael-Taktzir-EN.pdf

3. **ODNI [primary]**
   ICD 705, Sensitive Compartmented Information Facilities, 2010
   https://www.odni.gov/files/documents/ICD/ICD-705-SCIFs.pdf

4. **ODNI [primary]**
   ICD 906, Controlled Access Programs
   https://irp.fas.org/dni/icd/icd-906.pdf

5. **ODNI [primary]**
   ICD 704, Personnel Security Standards for SCI, 2008/2018
   https://www.odni.gov/files/documents/ICD/ICD-704-Personnel-Security-Standards-and-Procedures-for-Access-to-SCI-2018-06-20.pdf

6. **DCID 1/19 [primary]**
need-to-know definition
https://irp.fas.org/offdocs/dcid1-19.html

7. **Wikipedia**
Director of Security of the Defense Establishment [primary-adjacent reference]
https://en.wikipedia.org/wiki/Director_of_Security_of_the_Defense_Establishment

8. **Israel.com**
Gil Reich to Take Over the Defence Ministry's Security Arm, 2026-03-10
https://www.israel.com/news/defense-minister-israel-katz-decides-to-appoint-gil-reich-appointed-new-head-of-the-defense-security-directorate-at-israels-defense-ministry

9. **Mondoweiss**
Israeli Defense Ministry dep't is dedicated to covering up evidence of the Nakba, 2019-07-05 (reporting Haaretz)
https://mondoweiss.net/2019/07/ministry-dedicated-covering/

10. **Hikmah/Grotius**
Israel's Archives and Serious Crimes, 2021-12-18
https://www.hikmahs.org/israel-s-archives-and-serious-crimes

11. **Israel Defense**
on Shimoni's appointment and Malmab's legal regulation, 2021-11-01
https://www.israeldefense.co.il/node/52456

12. **Trach Law**
Security Clearance (Sivug Bitchoni) in Israel, 2026-06-07
https://trach-law.co.il/en/security-clearance-sivug-bitchoni-in-israel/