MY WEIRD PROMPTS

Podcast Transcript

EPISODE #376

Hardwired for Havoc: Inside Mossad’s Pager Operation

Published January 30, 2026 • Runtime: 29:28

https://myweirdprompts.com/episode/mossad-pager-supply-chain/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, hosts Corn and Herman Poppleberry deconstruct one of the most audacious and terrifying intelligence operations in modern history: the 2024 pager explosions in Lebanon. Moving beyond the immediate headlines, the duo explores the deep-cover logistics of "physical supply chain poisoning," explaining how Mossad spent nearly a decade establishing front companies to manufacture compromised hardware from the ground up. Herman breaks down the technical "nerdery" of how PETN explosives were integrated into battery packs without detection, while Corn highlights the psychological horror of a device that targets its user at the moment of highest attention. From the historical echoes of the CIA’s Crypto AG operation to the future of "zero-trust hardware," this episode is a gripping look at the death of trust in the global supply chain.

DANIEL'S PROMPT

Daniel

I'd like to discuss the recent Mossad beeper operation in Lebanon and specifically drill down into the use of front companies by intelligence agencies. How many years would Mossad have been planning an operation like this? I’d also like to explore the concept of physical supply chain poisoning and how it compares to traditional espionage techniques, like the 'man-in-the-middle' interception of mail, to understand how they successfully booby-trapped the hardware.

TRANSCRIPT

Corn

Welcome back to another episode of My Weird Prompts. I am Corn, and I am sitting here in our living room in Jerusalem with my brother, the man who probably has more tabs open on his browser than there are atoms in the observable universe.

Herman

Herman Poppleberry, at your service. And for the record, it is only forty-seven tabs today, Corn. I am practicing restraint.

Corn

Well, I hope one of those tabs is ready to go because our housemate Daniel sent us a prompt this morning that is, quite literally, explosive. He wants to talk about the M-O-S-S-A-D beeper operation in Lebanon.

Herman

Oh, man. Daniel really knows how to pick them. This is a masterclass in what we call physical supply chain poisoning. It is one of those stories that sounds like it was rejected from a James Bond script for being too unrealistic, yet it happened right in our backyard back in September of twenty twenty-four.

Corn

It is fascinating because it is such a perfect intersection of old-school espionage and high-tech interference. We have spent the last few episodes talking about digital threats, like the hidden cameras we discussed in episode three hundred sixty-eight, but this is something else entirely. This is reaching out and touching the physical world in a very permanent way.

Herman

Exactly. And Daniel specifically wanted to know about the front companies. How do you even begin to set up a shell corporation that can actually manufacture and ship thousands of devices without anyone smelling a rat?

Corn

Right. Because you cannot just open a shop on a street corner and start selling booby-trapped pagers to Hezbollah. There is a level of deep cover here that is staggering. So, Herman, let us start with the timeline. How many years are we talking about for an operation of this scale?

Herman

Most intelligence analysts suggest this was in the works for much longer than people realize. While the specific order for these pagers happened a few years before the blast, the infrastructure—the shell companies themselves—was being established as far back as around twenty fifteen. You have to remember, M-O-S-S-A-D did not just intercept a shipment of pagers. They created the entire supply chain from scratch. They established a company called B-A-C Consulting in Hungary. Now, on paper, this looked like a legitimate business. They had a website, a history of trading, and a C-E-O, Cristina Barsony-Arcidiacono, who had a resume that looked perfectly normal to a casual observer.

Corn

But they were not actually making anything in Budapest, were they?

Herman

Well, that is the clever part. They acted as a middleman. They secured a licensing agreement with a reputable Taiwanese company called Gold Apollo. This gave them the right to use the Gold Apollo brand name on the pagers. So, when the end-users in Lebanon looked at the devices, they saw a trusted, reputable brand from Taiwan. They did not see a shell company in Budapest or the secondary shell company, Norta Global, which was registered in Bulgaria to handle the actual money trail. It was a shell within a shell.

Corn

That is incredible. So they essentially outsourced the brand trust. It is like the ultimate version of white labeling, which we have touched on before. But instead of just putting your logo on a generic power bank, you are putting a reputable logo on a custom-built bomb.

Herman

Precisely. And the planning involves more than just the company. You have to build what spies call a legend. You need a paper trail of legitimate transactions. You need to pay taxes, you need to have employees who might not even know what the company is actually doing. You have to wait for the target to decide they need the product. In this case, Hezbollah made a strategic decision to move away from smartphones because they knew the Israeli signals intelligence was too good. They thought pagers were the safe, low-tech alternative.

Corn

It is the classic mistake of thinking that going backward in technology makes you invisible. They thought they were being clever by using nineteen-nineties technology, but they forgot that the physical device still has to come from somewhere.

Herman

Right. And that brings us to the actual poisoning. Daniel asked how this compares to the old man-in-the-middle mail interception. Back in the day, like we talked about in the episode regarding the history of the post office, intelligence agencies had these rooms called black chambers. They would steam open envelopes, read the letters, and reseal them so perfectly that the recipient never knew.

Corn

But doing that with a digital pager is a lot harder than steaming open a letter. You cannot just open thousands of boxes, unscrew the back of the pager, put in an explosive, and put it back together without leaving a trace. The weight would change, the internal components would look crowded on an X-ray. How did they actually pull off the hardware hack?

Herman

This is where the technical nerdery gets really intense. According to the forensic reports, the explosive material was not just shoved into the casing. It was integrated into the battery pack itself. They used a very small amount—approximately 3 to 10 grams—of a high explosive called P-E-T-N, which stands for pentaerythritol tetranitrate. They managed to disguise it as part of the battery cell or the circuit board during the actual manufacturing process.

Corn

Wait, so if you are a Hezbollah technician and you take one of these apart to check for bugs, what are you seeing?

Herman

You are seeing what looks like a standard lithium-ion battery. The explosive was likely thin and flat, hidden within the layers of the battery or the plastic casing. And because it was integrated during the manufacturing process by the front company, there were no tool marks. No scratched screws, no broken seals. It was manufactured to be a bomb from day one. This is the difference between interdiction—where you grab a box in the mail—and supply chain poisoning, where you are the one making the box.

Corn

That is the crucial difference. In the old days, you were tampering with a finished product. Here, the product was born compromised. It is like if the post office did not just read your mail, but they actually owned the paper factory and the ink company, so they could write whatever they wanted before the letter was even sent.

Herman

Exactly. And they even accounted for the weight. If you add explosive material, you have to remove an equivalent amount of something else to keep the weight identical to the official specifications. It is a level of detail that requires a massive engineering team. This was not a few guys in a basement. This was a state-level industrial project.

Corn

And the trigger mechanism? That had to be digital, right?

Herman

Yes. They sent a specific alphanumeric code. The pagers were programmed so that when they received this specific sequence of characters, it would trigger a short circuit in the battery, creating a spark that detonated the P-E-T-N. The brilliance, if you can call it that, was that the message itself looked like a normal notification. The pagers even beeped for several seconds before exploding, which caused the users to pick them up and look at them.

Corn

Which is why the injuries were so specific to the hands and faces. It is a psychological horror as much as a physical one. You take a device that is meant to keep you connected and turn it into a weapon that targets you when you are most attentive to it.

Herman

It really highlights the vulnerability of our global supply chain. We live in a world where we trust that the thing in the box is the thing on the label. But as we saw with the C-two-P-A discussion in episode three hundred sixty-six, proving reality is becoming harder and harder. In that episode, we talked about digital signatures for images. But how do you sign a physical circuit board?

Corn

That is the trillion-dollar question. If M-O-S-S-A-D can do this to a pager, what is stopping a nation-state from doing this to a router or a server or even a car? We have seen the N-S-A do something similar in the past, haven't we? Intercepting Cisco routers in transit?

Herman

Oh, absolutely. There are famous photos from the Edward Snowden leaks showing N-S-A technicians carefully opening Cisco boxes, installing what they called beacon firmware, and then resealing the boxes with factory tape. But that was interdiction. That was the man-in-the-middle. The Lebanon operation was a whole new level because they owned the factory. They were the manufacturer.

Corn

So, when Daniel asks about front companies, he is really asking about the death of trust in hardware. If a company can exist for years, build a reputation, and then deliver a poisoned product, how does any organization protect itself?

Herman

It is incredibly difficult. You have to move toward a model of zero-trust hardware. That means you do not trust the supplier, you do not trust the shipping company, and you do not trust the box. Some high-security government agencies actually buy their hardware anonymously from retail stores so that the supplier doesn't know who the end-user is. They will walk into a retail store and buy ten laptops off the shelf rather than ordering a custom batch from the manufacturer.

Corn

But even then, if the poisoning is at the factory level, like it was with B-A-C Consulting, buying off the shelf doesn't help you if the entire batch is compromised.

Herman

True. But in the M-O-S-S-A-D case, they were specifically targeting the supply line that they knew would end up with Hezbollah. They were not poisoning every Gold Apollo pager in the world. That would be too risky and would blow their cover immediately. They had to ensure that the poisoned units only went to their targets.

Corn

Which means they had to have people inside the logistics network. They had to know exactly which serial numbers were being shipped to which distributors. This is where the front companies become a web. You don't just have the manufacturer, you have the distributor, the freight forwarder, the customs agent.

Herman

And you can bet that M-O-S-S-A-D had eyes on every single one of those nodes. It reminds me of Operation Rubicon, which was one of the most successful intelligence operations in history. For decades, the C-I-A and the German intelligence agency, the B-N-D, secretly owned a Swiss company called Crypto A-G.

Corn

I remember you mentioning that once. They sold encryption machines to over a hundred countries, right?

Herman

Yes! And they rigged the machines so that the C-I-A could easily crack the codes. For forty years, countries like Iran, India, and Pakistan were paying millions of dollars to the C-I-A to buy machines that allowed the C-I-A to read their most secret messages. It is the same principle as the beeper operation, but for information instead of explosives.

Corn

It is the long game. I think that is what people struggle to grasp. We live in a world of twenty-four-hour news cycles, but intelligence agencies think in decades. Setting up a company around twenty fifteen to execute a strike in twenty twenty-four is just a standard Tuesday for them.

Herman

Exactly. And the level of patience required is insane. You have to let the target use the product safely for months or years. You have to build that sense of security. Hezbollah used those pagers for a long time before they were detonated. They had to believe they were safe. If one had gone off early by accident, the whole operation would have been ruined.

Corn

It makes me wonder about the second-order effects. Now that this has happened, every paramilitary group, every government, every corporation is looking at their hardware with total suspicion. Does this lead to a balkanization of hardware? Like, will China only use Chinese chips and the U-S only use U-S chips?

Herman

We are already seeing that, Corn. That is exactly what the whole Huawei and TikTok debate is about, at its core. It is about the fear of the kill switch. If you rely on a foreign power for your infrastructure, you have given them a weapon they can use at any time. The pager operation was just the most literal, violent expression of that fear.

Corn

It is funny, Herman, you mentioned the kill switch. In episode one hundred fifty-one, we talked about why your gigabit internet feels like dial-up, and we touched on how mesh networks are harder to shut down because they don't have a central point of failure. But here, the failure was distributed. The failure was in every single pocket.

Herman

That is a great point. Usually, you think of a supply chain attack as hitting a central server or a backbone. But this was a massively parallel attack. It was thousands of individual bombs. It is the ultimate nightmare for a security officer because there is no perimeter to defend. The threat is already inside the pocket of every one of your employees.

Corn

So, let us talk about the man-in-the-middle aspect again. Daniel mentioned the mail interception. In the digital world, we have things like H-T-T-P-S and end-to-end encryption to prevent people from reading our messages in transit. But there is no equivalent for physical objects. You can put a tamper-evident seal on a box, but as we know, those are surprisingly easy to fake.

Herman

They are. There are entire conferences where people show how to use heat guns and solvents to remove those void stickers without leaving a trace. And if the attacker is the one who made the sticker in the first place, well, you are out of luck. The only real solution is what is called destructive testing. You take a random sample of five percent of the shipment and you literally tear them apart. You dissolve the batteries in acid, you X-ray the circuit boards, you check every milligram of weight.

Corn

But even then, if you are a small organization, you don't have the resources to do that. Hezbollah is a large organization with a lot of funding, and they still missed it. It shows that even with a high level of suspicion, a well-executed front company can bypass almost any check.

Herman

And think about the legal and ethical gray zones here. These front companies are often registered in neutral countries or even allied countries. B-A-C Consulting was in Hungary, which is an E-U and N-A-T-O member. This puts the host country in a very awkward position. Did they know? Were they complicit? Or were they just as fooled as everyone else?

Corn

It creates this diplomatic friction that intelligence agencies love to exploit. They hide in the shadows of international trade law. It is much easier to ship a crate of pagers through an E-U port than it is to smuggle a crate of grenades across a border.

Herman

Absolutely. Pagers are dual-use technology. They are not weapons by definition. So they don't trigger the same export controls. This is the brilliance of the supply chain hack. You use the existing, frictionless pathways of global capitalism to deliver your payload.

Corn

So, looking forward, Herman, what is the takeaway for the average person? Obviously, we are not high-value targets for M-O-S-S-A-D, but this technology and these techniques eventually trickle down, don't they?

Herman

They do. We always see this. Military tech becomes intelligence tech, which becomes police tech, which eventually becomes criminal tech. The idea of hardware interdiction is already being used by sophisticated criminal groups to compromise point-of-sale terminals in retail stores. They will swap out a credit card reader with one that has a skimmer built into the hardware at the factory level.

Corn

So we are moving toward a world where you can't even trust the hardware you buy at the store. That is a depressing thought.

Herman

It is, but it also means we need to get smarter about transparency. There is a growing movement for open-source hardware. Just like we have open-source software where anyone can inspect the code, open-source hardware means the circuit designs and the bill of materials are public. If you can't verify the hardware, you shouldn't use it for anything sensitive.

Corn

But even then, someone has to manufacture the open-source design. You are still back to the factory problem.

Herman

True, but it is a lot harder to hide an explosive in a design that thousands of people are looking at. The complexity of modern electronics is the spy's best friend. There are so many tiny components in a smartphone or a pager that you can easily hide a few grams of something extra.

Corn

It reminds me of the old saying that any sufficiently advanced technology is indistinguishable from magic. In this case, any sufficiently advanced supply chain is indistinguishable from a conspiracy.

Herman

Ha! I like that. It is very Poppleberry. And it is true. We are so removed from the creation of our tools that we have to rely on a chain of trust that is thousands of miles long. And as M-O-S-S-A-D showed us, all it takes is one broken link, or one fake link, to change everything.

Corn

You know, thinking about the front companies again, it makes me wonder about the people who worked there. Imagine being a regular person in Budapest, getting a job as a secretary or a logistics coordinator for B-A-C Consulting. You think you are working for a tech startup, you go to work, you file paperwork, you order coffee for the office. And then one day you wake up and find out you were the civilian face of a massive lethal operation.

Herman

That is the real tragedy of the legend. To make a company look real, you have to involve real people. Most of the time, they are what spies call useful idiots. They are not in on the secret, but their presence provides the authenticity that fools the target. It is a cold, calculating way to use human lives.

Corn

It definitely adds a layer of moral complexity to the whole thing. It is not just about the targets in Lebanon; it is about the collateral damage to the idea of a peaceful, global society.

Herman

And it reinforces the need for skepticism. We talked about this in episode three hundred sixty-five regarding A-I memory. We are starting to outsource our trust to systems we don't understand. Whether it is an A-I model or a physical pager, if you don't know how it works and where it came from, you are vulnerable.

Corn

So, Daniel, if you are listening, I hope that answers your question. The front company isn't just a shell; it is a living, breathing organism designed to mimic a legitimate business until the moment it is needed. And the planning timeline? It is a marathon, not a sprint.

Herman

It is the ultimate long game. And I think we are going to be seeing the ripples of this for decades. It has changed the rules of engagement in a way that we are only beginning to understand.

Corn

Well, on that cheery note, I think it is time to wrap this up. Herman, do you have any final thoughts before we sign off?

Herman

Just that I am going to be looking at my old Nokia brick a lot more fondly today. It might not have apps, but at least I know it wasn't made by a shell company in Hungary.

Corn

Unless that is what they want you to think, Herman.

Herman

Don't start, Corn. My forty-seven tabs can't handle a new conspiracy theory right now.

Corn

Fair enough. Before we go, I want to say a huge thank you to all of you for listening to My Weird Prompts. We have been doing this for three hundred sixty-nine episodes now, and it is your curiosity that keeps us going. If you are enjoying the show, we would really appreciate it if you could leave us a review on Spotify or your favorite podcast app. It genuinely helps other curious people find the show.

Herman

It really does. And remember, you can find our full archive and a contact form at my weird prompts dot com. If you have a question that is keeping you up at night, send it our way. We love diving into these rabbit holes.

Corn

Thanks again to Daniel for the prompt. We will see you all next time. This has been My Weird Prompts.

Herman

Stay curious, and maybe double-check your batteries.

Corn

Goodbye, everyone!

Herman

Bye!

Corn

You know, I was just thinking, Herman. If we ever decided to start a front company, what would we sell?

Herman

Oh, definitely artisanal donkey treats. No one would ever suspect a donkey treat company.

Corn

I don't know, a donkey treat company run by a donkey and a sloth? That seems a bit on the nose.

Herman

Exactly! It is so obvious that it couldn't possibly be a cover. That is the genius of it.

Corn

I think you have been reading too many of those spy papers, Herman. Let us just stick to the podcast for now.

Herman

Fine, fine. But the offer stands if you ever want to get into the logistics business.

Corn

I will keep it in mind. See you at dinner.

Herman

See ya.

Corn

And to our listeners, one more time, thank you. We know there are a lot of podcasts out there, and the fact that you spend your time with us means the world. We will be back next week with another deep dive. Until then, keep asking the weird questions.

Herman

Because the weird questions usually have the most interesting answers.

Corn

Exactly. Signing off from Jerusalem. This is My Weird Prompts.

Herman

Peace out.