MY WEIRD PROMPTS

Podcast Transcript

EPISODE #140

Shadow Webs: The Secret Military Internet Explained

Published January 03, 2026 • Runtime: 24:17

https://myweirdprompts.com/episode/military-parallel-internet-security/

EPISODE SYNOPSIS

While we browse the civilian web, a parallel world of high-security "shadow" networks runs right beneath our feet and across the ocean floor. In this episode, Herman and Corn peel back the curtain on military infrastructure, explaining how systems like SIPRNet and DISN operate independently of our everyday internet. From the physical resilience of armored "dark fiber" and acoustic sensing to the ingenious use of data diodes and browser isolation, we explore how global powers maintain command and control in the most hostile environments. We also take a local look at Israel's Red Alert system to see these networks in action, proving that in the world of military tech, speed and security are matters of life and death. Tune in to learn why the most important parts of the internet are the ones you'll never see.

DANIEL'S PROMPT

Daniel

In our last episode, we discussed Operational Technology (OT), but I've always been curious about military networks. We've touched on systems like Israel's "Red Alert" and Command and Control (C2) networks, which are the backbone of military operations. Given the massive global footprint of something like the US military, how do governments and militaries actually go about creating and maintaining these networks? How is the physical infrastructure, like undersea cables, managed while keeping these systems air-gapped from civilian networks? Ultimately, how do these parallel internets work, and can you use standard tools like Google Chrome when connected to a military network?

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts! I am Corn, and as always, I am joined by my brother.

Herman

Herman Poppleberry, at your service. It is good to be back in the studio, Corn. We have a really fascinating prompt today from our housemate Daniel. He has been thinking about the literal foundations of the internet, but specifically the parts that most of us are never allowed to see.

Corn

Right, and it is a perfect follow up to last week, when we did episode two hundred forty five about the anatomy of the internet and those glass threads. Daniel was asking about military networks. We are talking about the parallel internets that run alongside our civilian web, but are fundamentally different in how they are built, managed, and secured.

Herman

It is such a deep rabbit hole. When people think of the internet, they think of this singular, global cloud. But in reality, the military and intelligence communities operate on what we call air gapped or multi level security networks. The United States military, for example, has the Defense Information Systems Network, or DISN. And within that, you have different flavors like NIPRNet for unclassified stuff and SIPRNet for secret level data.

Corn

I think the most striking thing for me, and Daniel touched on this in his prompt, is the sheer physical scale. If the US military has a global footprint with hundreds of bases, how do they actually connect them without just piggybacking on the same fiber cables that carry my Netflix traffic? Or do they?

Herman

That is the million dollar question. The answer is a bit of a hybrid, but it is heavily tilted toward private infrastructure. The military does not just lease a line from a local internet service provider in every country. For their core backbone, especially the transoceanic stuff, they often own their own fiber or they lease what we call dark fiber.

Corn

Dark fiber, meaning the physical glass is there but the civilian provider is not the one putting the light through it?

Herman

Exactly. They buy the rights to use the physical strand of glass and then they attach their own highly encrypted, military grade hardware at both ends. This gives them total control over the data link layer. But even more interesting is how they manage the undersea portion. You might remember from our previous episodes that there are only a few hundred major undersea cables connecting the world. The military often secures capacity on these through secret agreements, or in some cases, they have their own dedicated spurs.

Corn

But wait, if they are using the same physical cable as everyone else, even if it is a different fiber strand, does that not make it vulnerable? If a ship drags an anchor and snaps the cable, does the military lose its connection just like the rest of us?

Herman

To some extent, yes, physical reality is the ultimate bottleneck. But the military builds in massive redundancy. They use a mesh architecture where data can be rerouted through satellites or different geographic paths instantly. And speaking of satellites, that is a huge part of the military internet. While we are starting to get used to things like Starlink, the military has had its own high bandwidth constellations for decades. They use these to bridge the gaps where fiber is not feasible.

Corn

I want to pivot to the local context here in Jerusalem, because Daniel mentioned the Red Alert system. We have all experienced those moments where the sirens go off and the app on our phone pings almost simultaneously. That is a perfect example of a military network interfacing with a civilian one. How does that command and control, or C2, actually function in real time?

Herman

It is an incredible feat of engineering. Think about the latency requirements. From the moment a radar system detects a launch to the moment your phone vibrates, we are talking about seconds. The radar data is processed on a high speed military backbone, which then triggers the sirens directly through a dedicated radio frequency network. It does not rely on the civilian internet for the sirens themselves because that would be too slow and too unreliable. The smartphone app is a secondary layer that pulls from a government API, but the core system is its own isolated beast.

Corn

That makes sense. You cannot have a siren waiting for a 5G signal to buffer. But what about the air gapping Daniel mentioned? He asked how they keep these systems separate. If the Red Alert system is sending data to a civilian app, is there not a bridge there?

Herman

There is a bridge, but it is a one way bridge. In the world of cybersecurity, we call these data diodes. It is a piece of hardware that physically only allows data to travel in one direction. Think of it like a valve. Information can flow from the secure military side out to the civilian side, but nothing can go back the other way. This prevents a hacker on the public internet from using the app connection to crawl back into the military command and control servers.

Corn

That is a great analogy. A one way valve for data. But Daniel also brought up something more old school, the pagers. We saw that recent news about groups like Hezbollah reverting to pagers to avoid signal intelligence. It feels like the ultimate air gap is just going back to nineteen ninety four technology.

Herman

It really is. It shows that the more sophisticated the network, the more points of failure or interception you create. If you are using a modern smartphone, you have GPS, you have a microphone, you have a camera, and you are constantly pinging cell towers. A pager is a passive receiver. It just listens for a broadcast. It does not talk back, which makes it incredibly hard to geolocate. But as we saw, even that has physical supply chain vulnerabilities.

Corn

It is like a game of cat and mouse where the mouse decides to stop using the fancy electronic cheese detector and just uses its nose, but then the cat poisons the cheese itself.

Herman

Exactly. And that leads into the software side of things. Daniel asked if you can use Google Chrome on a military network. The answer is actually yes, but it is not the Chrome you and I know.

Corn

Wait, really? I pictured them using some green text on a black screen from the nineteen eighties.

Herman

Oh, they definitely have plenty of that in the older systems, but for daily work, they use modern browsers. However, they are what we call hardened versions. In a secure environment, the browser might be running in a virtual machine that is wiped clean every time you close the tab. Or, more commonly, they use something called browser isolation. The actual website is being rendered on a server far away, and it just sends a safe picture of the website to the user's screen.

Corn

So if I clicked on a malicious link, the virus would just infect a temporary server in a data center and then vanish when I logged off?

Herman

Precisely. And they often disable things like extensions, certain types of JavaScript, and definitely anything that tries to call home to a third party tracking server. It is a very sterile experience. You are not going to be seeing targeted ads for new shoes while you are looking at satellite imagery of a naval base.

Corn

That sounds like a dream, actually. An internet without ads. But I suppose the trade off is that you are probably being monitored by your own superiors every second.

Herman

Every single keystroke. On those networks, there is no expectation of privacy from the organization. It is all about mission security. But let's take a quick break before we dive deeper into the physical cables and how they actually lay these things across the ocean floor. We have a word from our sponsor.

Corn

Let's take a quick break from our sponsors. Larry: Are you worried about the government listening to your thoughts through your microwave? Are you tired of your neighbors stealing your Wi-Fi signals with their brains? Introducing the Faraday Fedora! It is not just a stylish hat, it is a personal fortress for your cranium. Lined with a proprietary blend of aluminum, copper, and recycled gum wrappers, the Faraday Fedora blocks ninety nine point nine percent of all incoming and outgoing psychic frequencies. Whether it is 5G, 6G, or the local weather report, your thoughts stay where they belong, inside your head! Available in three colors: Tin Foil Silver, Stealth Charcoal, and Paranoid Polka Dot. The Faraday Fedora, because if you can hear them, they can definitely hear you. BUY NOW!

Corn

Alright, thanks Larry. I think I will stick to my regular baseball cap for now. Anyway, Herman, back to the serious stuff. We were talking about the physical infrastructure.

Herman

Right. One thing Daniel asked was how militaries manage these networks globally. The US military, for instance, has a massive operation called the Army Signal Corps. These are the people whose entire job is to build and maintain the internet where the internet does not exist. If they set up a base in the middle of a desert, they are not waiting for the local cable company to show up. They are deploying tactical satellite terminals and laying their own fiber in trenches.

Corn

I remember when we talked about the last mile in episode forty, regarding AliExpress deliveries here in Israel. The military has a similar last mile problem, but instead of packages, it is life or death data. How do they ensure that the line does not get cut by a literal shovel?

Herman

They use armored cable. Military fiber optic cable is often wrapped in steel wire or high strength aramid fibers, which are the same materials used in bulletproof vests. It is designed to be run over by tanks and still function. And they use something called acoustic sensing. They can actually use the fiber optic cable itself as a giant microphone.

Corn

Wait, the cable is the microphone? How does that work?

Herman

It is a technology called Distributed Acoustic Sensing, or DAS. They send pulses of light down the fiber, and if someone starts digging near the cable, the vibrations cause tiny changes in how the light bounces back. By analyzing those reflections, they can tell exactly where the digging is happening, down to a few meters. They will know you are there before you even hit the dirt.

Corn

That is incredible. So the network is self aware in a physical sense. It knows when it is being messed with.

Herman

Exactly. And that level of monitoring extends to the undersea cables too. There have been reports for years about specialized submarines designed to tap into these cables or to protect them. The US Navy has the Jimmy Carter, which is a highly modified submarine believed to be capable of performing maintenance or potentially intercepting data on the ocean floor.

Corn

This brings up a point Daniel mentioned about private companies like Google and Meta laying their own cables. If the world's data is moving onto private infrastructure, does the military lose its edge? Or do they just become the biggest customers of Google's cables?

Herman

It is a bit of both. The trend is definitely toward using commercial infrastructure for non sensitive data because it is cheaper and faster. But for the core command and control stuff, the military will always want their own dedicated, sovereign paths. The risk of a private company being compromised or simply turning off the tap during a conflict is too high.

Corn

So we really do have two parallel worlds. There is the one we are in right now, recording this and eventually uploading it to Spotify, and then there is this shadow version that is tougher, faster, and completely invisible to us.

Herman

It is a shadow world that provides the foundation for our world. Without those high speed military alerts and the security they provide, our civilian internet would be much more vulnerable to disruption. But let's talk about the practical side for a second. If you were a soldier and you wanted to check your personal email, would you do that on the same computer where you look at secret maps?

Corn

I would hope not. I assume that is where the air gap comes in.

Herman

Precisely. In many military offices, you will see two different computers on one desk. One is connected to the NIPRNet, which is the unclassified network where you can access the regular internet, check your email, and maybe even watch a training video on YouTube. The other computer is connected to the SIPRNet or an even higher level network. These two computers are physically separated. They don't share a keyboard, they don't share a mouse, and they definitely don't share a cable.

Corn

Is there any way to move a file from one to the other? Like, if I have a really important PDF on the unclassified side that needs to go to the secret side?

Herman

That is where the term sneaker net comes from. In the old days, you would put it on a floppy disk or a CD and walk it over. But today, that is a huge security risk. Remember the Stuxnet virus? That was reportedly spread via a USB drive into an air gapped facility. So now, most military branches have extremely strict rules about removable media. To move a file, you usually have to go through a secure transfer gateway where the file is scanned, stripped of any hidden code, and then basically re created on the other side.

Corn

It sounds like a massive headache. It makes you realize how spoiled we are with our seamless cloud syncing and airdropping.

Herman

It is a headache by design. Security is the enemy of convenience. If it is easy for you to move a file, it is easy for a spy to move a file.

Corn

Let's talk about the future of this. We are in early twenty twenty six now. We are seeing AI being integrated into everything. How is that changing these military networks? Are they building AI that can manage the network traffic autonomously?

Herman

Absolutely. We are seeing the rise of what is called self healing networks. If a cable is cut or a satellite is jammed, the AI can instantly calculate the most efficient new path for the data and reconfigure the routers across the globe in milliseconds. It is much faster than a human operator could ever react. And they are using AI for anomaly detection. If a single user starts downloading data in a pattern that looks slightly off, the AI can lock down that terminal before the person even finishes their sentence.

Corn

It feels like the network itself is becoming a sentient bodyguard.

Herman

That is a good way to put it. But it also creates new risks. If an adversary can trick the AI into thinking there is a failure where there isn't one, they could potentially steer military traffic into a trap or a bottleneck. It is the new frontier of electronic warfare.

Corn

So, to go back to Daniel's original curiosity, the military internet is not just a faster version of ours. It is a fundamentally more paranoid and more robust version. It uses the same physics, the same IP protocols, and sometimes even the same browsers, but the way it is wrapped in layers of physical and digital armor makes it a different species entirely.

Herman

Exactly. It is the difference between a civilian car and an armored personnel carrier. They both have four wheels and an engine, and they both drive on the same roads, but one is built to survive a landmine and the other is built to get you to the grocery store.

Corn

That is a perfect analogy. So, what are the practical takeaways for our listeners? I mean, most of us will never log into SIPRNet. But how does understanding this help us?

Herman

I think the first takeaway is an appreciation for the physical reality of the internet. When your Wi-Fi is slow, remember that there are literal glass threads under the ocean being guarded by submarines. The second takeaway is about your own security. If the military thinks it is necessary to physically separate their computers to stay safe, maybe we should be a little more careful about what we click on and how we manage our own data. You might not need an air gap, but a little bit of digital hygiene goes a long way.

Corn

And maybe don't use a pager if you're worried about someone intercepting your messages, unless you really like that ninety's aesthetic.

Herman

Well, and as we saw, even the low tech stuff has a supply chain. True security is about knowing every link in the chain, from the factory to the browser.

Corn

This has been such an eye opening discussion. It really makes you look at the world differently. Every time I see a siren on a building now, I'm going to be thinking about that dedicated radio network and the radar systems talking to each other in the background.

Herman

It is all around us, Corn. The invisible architecture of the modern world.

Corn

Well, I think that covers a lot of ground. Daniel, thanks for sending in that prompt. It definitely took us down a deeper path than I expected.

Herman

Yeah, it was a great one. And hey, if any of you listening out there are enjoying these deep dives into the weird and wonderful parts of our world, we would really appreciate it if you could leave us a review on Spotify or whatever podcast app you use. It genuinely helps other people find the show and keeps us going.

Corn

Absolutely. We love hearing from you. You can also visit our website at myweirdprompts.com. We have the full archive there, including that episode on AliExpress we mentioned, and a contact form if you have a weird prompt of your own.

Herman

We are always looking for new rabbit holes to explore. Until next time, I am Herman Poppleberry.

Corn

And I am Corn. This has been My Weird Prompts.

Herman

Stay curious, everyone.

Corn

And keep an eye on those glass threads. See you next week!

Herman

Bye now! Larry: BUY NOW!