Podcast Transcript

EPISODE #334

Subsea Secrets: How AI Taps the World's Fiber Optics

Published January 28, 2026 • Runtime: 21:57

https://myweirdprompts.com/episode/underwater-cable-surveillance-ai/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, Herman and Corn Poppleberry dive deep into the hidden world of signals intelligence (SIGINT) to answer a heavy-hitting prompt from their housemate, Daniel. They pull back the curtain on the physical infrastructure of the internet, exploring how 99% of global traffic flows through subsea fiber optic cables and how governments utilize "Infrastructure Sovereignty" to monitor these lines. From the mechanics of passive optical splitters at cable landing stations to the rise of Agentic AI for real-time data triage, the brothers explain how modern surveillance has moved beyond targeted wiretaps to a model of total information awareness. They also discuss the chilling reality of "Harvest Now, Decrypt Later" strategies and the legal loopholes of the Five Eyes alliance. This is a must-listen for anyone curious about the "plumbing" of global surveillance and the digital fingerprints we leave behind in a world where metadata is more valuable than content.

DANIEL'S PROMPT

Daniel

I would like to discuss signals intelligence and the large-scale ingestion of internet traffic by governments. Given what we know about networking infrastructure like underwater cables, how does the process of targeting and processing internet traffic at scale actually work? If a major Western democracy were to provide a briefing on their methods for signals intelligence gathering, what would they tell us?

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. It is January twenty-eighth, twenty twenty-six, and we are diving into the deep end today. I am Corn, and I am joined as always by my brother, the man who probably has an actual fiber optic map of the Atlantic Ocean floor tattooed on the inside of his eyelids.

Herman

Herman Poppleberry, at your service. And Corn, you are not far off. Our housemate Daniel sent us a absolute heavy hitter of a prompt today. He wants to know about the actual, gritty mechanics of signals intelligence at scale. Specifically, how do governments ingest the entire internet through underwater cables, and what would a real, classified briefing on these methods actually look like if the curtains were pulled back?

Corn

It is such a fascinating question because most people still think of surveillance as this targeted, James Bond style thing where you tap one specific phone or bug a single hotel room. But in twenty twenty-six, the scale is just unimaginable. We are talking about drinking from a firehose that puts out petabytes of data every single hour. It is not about finding a needle in a haystack anymore; it is about digitizing the entire hay field and using AI to tell you which straw looks suspicious.

Herman

Exactly. And Daniel really hit on the right starting point: the plumbing. If you want to understand signals intelligence, or SIGINT, you have to start with the physical infrastructure. About ninety-nine per cent of all international data—your emails, your video calls, your banking transactions, and even this podcast—travels through fiber optic cables resting on the ocean floor. They are the literal nervous system of the global economy.

Corn

And what is wild is how much that plumbing has changed just in the last few years. It used to be all telecommunications consortiums—groups of phone companies getting together to share the cost. But now, tech giants like Meta and Google are essentially the ones laying the pipes. Google has the Firmina cable running from the United States to Chile, and 2Africa is a consortium project with Meta participation that's approximately 37,000 kilometers long. When you own the transmission lines, you own the terrain. Herman, if we were in a briefing right now, how would they describe the importance of this ownership?

Herman

They would call it "Infrastructure Sovereignty." If a major Western democracy were giving you this briefing, the first slide would be a map of these cables. They would explain that the physical path a packet takes determines which laws apply to it. If your data from Brazil to Portugal happens to hop through a landing station in Virginia, it is suddenly subject to United States surveillance laws. The briefing would emphasize that the goal is to ensure as much global traffic as possible touches "friendly" soil.

Corn

And that brings us to the actual points of ingestion. These cables are not just endless loops of glass. They have to come up for air eventually. Herman, talk to me about Cable Landing Stations. In twenty twenty-six, these are not just small huts on a beach, right?

Herman

Not at all. These are five-megawatt digital command centers. They are some of the most heavily guarded civilian infrastructures on Earth. Think high-fences, biometric scanners, and twenty-four-seven monitoring. This is where the actual "tapping" happens. In our hypothetical briefing, this is where they would introduce the two primary methods of collection: "outside-in" and "inside-out."

Corn

I love the name "outside-in." It sounds like someone trying to break into a house, whereas "inside-out" sounds like the house itself is working against you.

Herman

That is a perfect analogy. "Outside-in" is the physical interception of the signal. To do this, you use something called a passive optical splitter. Usually, these are planar lightwave circuit, or PLC splitters. They are ingenious because they use the physical properties of light to divide a single beam into multiple paths. Imagine a prism. You take the light coming off the fiber optic cable and you split it, maybe in a ninety-nine to one ratio.

Corn

And that one per cent is all you need?

Herman

More than enough. Ninety-nine per cent of the light continues on its merry way to the destination, so the person on the other end never notices a thing. But that one per cent of the signal is diverted into a government-controlled server rack located right there in the landing station or piped via a dedicated line to a central processing facility. And because it is a passive splitter, it does not require power and it does not introduce a delay that a network engineer would easily spot. It is essentially a silent mirror.

Corn

But "inside-out" is where the real twenty twenty-six paranoia kicks in. That is when the interception capability is baked into the hardware itself. We are talking about exploits at the firmware level in the routers, switches, and even the repeaters that sit every fifty kilometers under the sea to boost the signal.

Herman

Precisely. If you control the switch, you do not need a physical splitter. You just tell the software to "blind carbon copy" every packet that matches a certain criteria and send it to a different IP address. This is why the geopolitical tension over companies like China's HMN Tech is so high. If a country suspects the repeaters on the ocean floor have a "management plane" backdoor, they realize they have lost control of the data before it even hits the beach.

Corn

So, we have the data diverted. It is flowing into the government's hands. Now we hit the "at scale" part of Daniel's prompt. Herman, help me with the math here. If we are talking about the entire internet, how do you even begin to process that much information?

Herman

It is a staggering engineering challenge. We know from historical data that an agency like the National Security Agency might "touch" vast amounts of global internet traffic. In twenty twenty-six, with the global internet handling around five to ten zettabytes of data a year, the scale is still tens of petabytes every single day. You cannot store all of that. No one has enough hard drives, and even if you did, you could never search it fast enough.

Corn

So, the briefing would have to explain the triage process. How do they decide what to keep and what to throw away in real-time?

Herman

This is where the technology has really leaped forward in the last two years. They use something called "Agentic AI" for real-time triage. In the past, you had static filters. You would look for "strong selectors" like an email address, a phone number, or a specific IP address. If a packet matched, you kept it. If not, it was discarded after a few hours. But static filters are easy to evade. You just change your email or use a different IP.

Corn

But Agentic AI is not just looking for a string of text, right? It is looking for the "vibe" of the data.

Herman

In a way, yes. These AI agents are performing behavioral analytics at line speed—we are talking terabits per second. They are looking for patterns. Is this encrypted traffic behaving like a standard Netflix stream, or is it showing the hallmarks of a command-and-control signal for a botnet? The AI agents can synthesize context across multiple streams. It might see an anomaly in a financial transaction in London and correlate it with a burst of encrypted traffic from a server in Singapore, all in milliseconds. It creates a "risk score" for every session. If the score is high enough, the system triggers a full capture.

Corn

So the "briefing" would basically tell us that they are moving away from "collecting everything" and toward "analyzing everything to decide what to collect."

Herman

Exactly. It is a shift from a library model to a triage model. They use massive data buffers, essentially high-speed memory banks, that hold the traffic for a few seconds or minutes. During that window, the AI agents do a "pre-selection." They tag the traffic with metadata: who, when, where, and how long. Even if they discard the actual content of your video call, they keep the metadata forever.

Corn

And we have to talk about metadata, because that is the part people always underestimate. They think if their message is encrypted, they are invisible. But the metadata is often more valuable to an intelligence agency than the actual content. Herman, remind me of that famous quote from the former NSA director.

Herman

Michael Hayden. He said, "We kill people based on metadata." It sounds cold, but from a technical perspective, it is a statement of fact. If I know that you called a known associate of a foreign intelligence service at three in the morning every day for a week, and then you both traveled to the same coordinates in a third country, I do not need to know what you said to have a very good idea of what is happening. Metadata allows them to build a "social graph" of the entire world. It maps the relationships between every person, device, and organization.

Corn

And in twenty twenty-six, with the Internet of Things, that graph is denser than ever. Your smart watch, your car's telemetry, even your smart fridge—they are all leaking metadata into that underwater cable firehose. It is a digital fingerprint that you leave on everything you touch.

Herman

And that brings us to one of the most controversial parts of any modern SIGINT briefing: the "Harvest Now, Decrypt Later" strategy. This is a critical concept for Daniel's question. Even if the government cannot break your encryption today, they might still store the encrypted blob of data if they think you are an important target.

Corn

Because they are waiting for the "Quantum Leap."

Herman

Exactly. NIST finalized initial Post-Quantum Cryptography standards in 2024, and governments and big tech are progressively implementing them into 2026 and beyond. But the intelligence agencies have been collecting encrypted data for a decade, betting that a cryptographically relevant quantum computer will eventually be able to crack it. If you sent a sensitive document in twenty twenty-one using old RSA encryption, it is sitting in a data center in Utah right now, just waiting for the hardware to catch up.

Corn

It is a sobering thought. Your secrets today are just on a timer. If a Western democracy were being truly honest in a briefing, they would tell you that the goal of signals intelligence is "total information awareness." They want to be able to reconstruct the digital life of a target retrospectively. They do not just want to know what you are doing now; they want to be able to go back five years and see who you were talking to before you were even on their radar.

Herman

That retrospective capability is the "holy grail." When everything is recorded and indexed by metadata, time becomes a dimension you can just scroll through. But we have to talk about the "wrapper" around all of this: the legal frameworks. In a briefing, they would spend a lot of time on Section seven hundred and two of the Foreign Intelligence Surveillance Act in the United States, which was reauthorized in April 2024 for two years.

Corn

Right, and they always emphasize that they are "targeting" non-citizens outside the country. That is the legal hook that allows them to bypass the standard warrant requirements that would apply to a domestic investigation.

Herman

But as we know, "incidental collection" is the massive loophole. If I am in London and I email a friend in New York, and that email happens to pass through a server that is being monitored because of a different target, my data gets "incidentally" scooped up. Once it is in the system, it can be searched. And then you have the "Five Eyes" alliance—the United States, United Kingdom, Canada, Australia, and New Zealand.

Corn

The ultimate data-sharing club. "I didn't spy on my citizen, but my partner in Australia happened to intercept their traffic, and they were kind enough to share it with me."

Herman

It is a very convenient arrangement. Although, in twenty twenty-six, we are seeing some real friction in that alliance. There have been reports out of Canada and Australia about foreign interference reaching into their own intelligence services. It has made the partners very nervous about what they share. Trust is the coin of the realm. If you cannot trust your partner to keep the source of the intelligence secret, the whole system starts to fracture.

Corn

So, if we look at the "briefing" Daniel asked for, it would be this weird mix of "here is the incredible technology we use to keep the world safe" and "here are the strict legal boundaries we follow." But the technical reality is that the boundary between "targeted" and "mass" surveillance is thinner than a single strand of fiber optic glass.

Herman

It really is. So, what does this mean for the average person? If the scale of ingestion is this massive, and the AI is this smart, is privacy even possible?

Corn

It feels like a "cat and mouse" game that the mouse is losing. The move to Post-Quantum Cryptography is a big step, though. If you are using apps that have already migrated to PQC—like Signal or the updated versions of iMessage—you are much safer from that "Harvest Now, Decrypt Later" threat. But even then, the metadata still exists. Your phone still has to talk to a cell tower. Your router still has to send packets to an IP address.

Herman

Exactly. You can hide the "what," but it is almost impossible to hide the "fact" of the communication. VPNs help to an extent, but you are really just shifting your trust from your internet service provider to a VPN company. And if that VPN company's traffic is passing through one of those landing stations we talked about, the government still sees that "IP address A" is talking to "VPN server B."

Corn

It feels like the only way to be truly private is to go completely off-grid, but even then, satellite intelligence is so advanced now that they can probably see the steam rising from your coffee cup in the middle of the woods.

Herman

Probably. But for most people, the takeaway is about risk modeling. Signals intelligence at scale is primarily looking for "needles." Unless you are doing something that triggers those agentic AI triage bots—like communicating with known high-risk entities or exhibiting very specific anomalous behaviors—you are just part of the background noise. You are one pulse of light in a zettabyte of data.

Corn

Background noise. That is a comforting, if slightly depressing, way to think about our digital lives. We are all just ghosts in the machine, or rather, pulses in the cable.

Herman

It is the reality of the twenty-six zettabyte era. We are all just data points at the bottom of the ocean.

Corn

Well, on that poetic note, I think we have given Daniel plenty to chew on. The scale is massive, the tech is agentic, and the ocean is full of prisms and backdoors. It is a wild world under the waves.

Herman

It really is. And hey, if you are listening and you have a thought on this—or maybe you work at a Cable Landing Station and want to give us an "anonymous" tour of the server room—get in touch at myweirdprompts.com. We have a contact form there, and we love hearing from you.

Corn

We really do. And if you have been enjoying our deep dives into the weird and the wired, please take a second to leave us a review on Spotify or wherever you listen. It genuinely helps the show grow and helps other curious minds find us. We are available on Spotify and the website, where you can also find our full archive and RSS feed.

Herman

This has been My Weird Prompts. I am Herman Poppleberry.

Corn

And I am Corn. Thanks for hanging out with us in the deep end today. Until next time.

Herman

See ya!