MY WEIRD PROMPTS

Podcast Transcript

EPISODE #214

Undersea Cables: The Fragile Backbone of the Global Web

Published January 10, 2026 • Runtime: 23:05

https://myweirdprompts.com/episode/undersea-internet-backbone-security/

EPISODE SYNOPSIS

While we often imagine the internet as an ethereal cloud, the reality is a physical network of glass fibers resting on the ocean floor. In this episode, Herman and Corn discuss the extreme vulnerabilities of these undersea cables, from accidental anchor drags to high-tech submarine tapping by global superpowers. We explore why HTTPS isn't a total shield against metadata analysis and how the "store now, decrypt later" strategy is driving a shift toward post-quantum cryptography. Join us as we dive into the murky world of deep-sea surveillance and the geopolitical battle for the internet’s physical foundation.

DANIEL'S PROMPT

Daniel

"I'd like to discuss the internet backbone, specifically undersea cables, as a potential vulnerability. Since most internet data is encrypted via HTTPS, is that data actually safe? Why are governments like Russia and China reportedly surveying and mapping these cables? Let's explore the security dimensions of the internet backbone."

TRANSCRIPT

Corn

Hey everyone, welcome back to 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 in his brain than a Chrome browser on a busy Monday.

Herman

Herman Poppleberry, present and accounted for. And you are not wrong, Corn. My brain is definitely hitting some high memory usage today, especially after the prompt our housemate Daniel sent over. He has been thinking about the literal, physical foundations of the internet.

Corn

It is funny because we spend so much time talking about the cloud, or wireless protocols, or the software layer. We discussed BGP and satellite rebels back in episode two hundred and nine, but Daniel’s prompt today is much more... grounded. Or, I guess, watered down? He is asking about the undersea cables that form the internet backbone.

Herman

It is a fascinating rabbit hole. Daniel mentioned that video of the IT manager in Denmark holding a fiber optic cable and saying he was holding half of the country’s internet in his hand. That is not hyperbole. That is the reality of our global infrastructure. We have this illusion of a wireless, ethereal world, but it is all anchored to the sea floor by glass and light.

Corn

And the core of his question is really about vulnerability. If these cables are the lifeblood of the global economy and communication, how safe are they? Especially when we hear reports about countries like Russia or China mapping them out. Does HTTPS even matter if someone can just... tap into the pipe at the bottom of the ocean?

Herman

That is exactly where we need to start. Because there is a huge difference between breaking the pipe and reading the water flowing through it. But before we get into the spy craft and the geopolitics, we should probably establish the scale of what we are talking about. People often think the internet is mostly satellites now, thanks to things like Starlink.

Corn

Right, but that is a tiny fraction of the traffic, isn't it?

Herman

It is negligible for the global backbone. Roughly ninety-five to ninety-nine percent of international data is carried by subsea cables. As of early twenty twenty-six, we are talking about over five hundred subsea cables stretching over roughly one point four to one point five million kilometers. To put that in perspective, that is enough cable to wrap around the Earth around thirty-five times.

Corn

That is incredible. And these aren't massive pipes, right? Daniel mentioned they are about the size of an Ethernet cable, or maybe a garden hose?

Herman

In the deep ocean, where they are less likely to be disturbed, they are surprisingly thin. About twenty-five millimeters in diameter. Most of that is protective casing. The actual fiber optic strands that carry the data are as thin as a human hair. As you get closer to the shore, they get much thicker, wrapped in layers of steel wire and plastic to protect them from anchors and fishing nets. But the heart of it is just light traveling through glass.

Corn

Okay, so let's tackle the security aspect. Daniel’s first big question: is our data safe because of HTTPS? If I am sending an encrypted message from here to New York, and it travels through one of these cables, and a hostile actor has a tap on that cable, can they see what I am saying?

Herman

The short answer is no, they cannot read the content of your message, but the long answer is much more concerning. HTTPS, or more accurately TLS, which stands for Transport Layer Security, encrypts the payload. If someone taps the cable, they see a stream of seemingly random bits. They don't have the private keys to decrypt it. However, they can see the metadata.

Corn

Right, we have talked about metadata before. That is the who, when, and where, even if they don't know the what.

Herman

Exactly. Even with encryption, a sophisticated actor can see the source IP address, the destination IP address, and the volume of data. If they are monitoring the entire cable, they can perform traffic analysis. They can see that a specific person in Jerusalem is communicating with a specific server in Virginia at a specific time. In the world of intelligence, sometimes the fact that a conversation is happening is more important than the words being said.

Corn

And there is also the store now, decrypt later strategy, right?

Herman

That is the big boogeyman in the room. If a government is tapping a backbone cable, they can record massive amounts of encrypted data. They might not be able to break it today, but they are betting on the fact that in ten or fifteen years, quantum computers will make today's encryption trivial to crack. This is why the transition to Post-Quantum Cryptography, or P-Q-C, is so critical right now. The standards were finalized by NIST back in twenty twenty-four, but the rollout across the global backbone is still a work in progress.

Corn

That is a sobering thought. But how do you even tap a cable at the bottom of the ocean? I mean, we are talking about thousands of meters of pressure. You can't exactly go down there with a pair of wire cutters and a laptop.

Herman

It is incredibly difficult, which is why only a few nations have the capability. You need specialized submarines. The United States has the USS Jimmy Carter, which is a modified Seawolf-class submarine specifically designed for undersea research and, well, covert operations. It has a dedicated section for divers and remotely operated vehicles to work on the sea floor.

Corn

And what are they actually doing? Are they physically cutting into the fiber?

Herman

Not usually. If you cut the fiber, the light stops, and the operators at the landing stations know immediately. They can use a technique called Optical Time-Domain Reflectometry to pinpoint the break within meters. No, to tap it secretly, you use something called a non-invasive optical tap. You bend the fiber just enough so that a tiny bit of light leaks out of the cladding. You capture that leaked light, amplify it, and you have a copy of the signal without ever interrupting the flow of data.

Corn

That sounds like something out of a James Bond movie. But Daniel mentioned Russia and China specifically. Why are they surveying these areas? Is it just about tapping, or is there something more destructive in mind?

Herman

This is where we get into the concept of hybrid warfare. If you want to paralyze a modern nation, you don't necessarily need to drop bombs. You just need to cut their connection to the global economy. Imagine if the cables connecting the United Kingdom to the United States were suddenly severed. The financial markets would freeze, GPS-dependent systems might struggle with timing synchronization, and communication would collapse.

Corn

I remember reading about the Russian ship, the Yantar. It is officially an oceanographic research vessel, but NATO has been tracking it for years because it has a habit of researching right on top of critical internet cables.

Herman

Precisely. The Yantar carries deep-sea submersibles that can stay on the sea floor for long periods. The fear isn't just that they are tapping the cables, it is that they are mapping the exact locations and vulnerabilities so that in the event of a conflict, they can cut them. And here is the kicker,

Corn

the cables are often clustered together in certain geographic choke points.

Corn

Like the Strait of Malacca or the Suez Canal?

Herman

Exactly. Or the Luzon Strait between Taiwan and the Philippines. If you look at a map of undersea cables, you see these massive bundles of lines all passing through the same narrow corridors. A single well-placed submarine or even a rogue fishing trawler with a heavy anchor could take out a significant portion of a continent's bandwidth in one go.

Corn

This reminds me of our discussion in episode one hundred and seventy-three about achieving the gold standard of uptime. We talked about redundancy. Don't these cables have built-in redundancy? If one goes down, doesn't the traffic just reroute?

Herman

It does, but only if there is spare capacity on the other routes. The internet is designed to be resilient. If a cable in the Atlantic breaks, traffic might be rerouted through the Pacific or across land lines through Asia. But that causes massive latency spikes and congestion. And if you take out multiple cables in a coordinated attack, there simply isn't enough pipe elsewhere to handle the load.

Corn

It is a fragile equilibrium. And it is not just about state actors, right? Didn't a ship's anchor once take out the internet for a huge part of Africa?

Herman

Yes, several times! In twenty twenty-four, we saw multiple cables in the Red Sea damaged near the last known position of the cargo ship Rubymar after it was attacked, and analysts have suggested its anchor as a possible cause. It took months to repair because you can't just send a repair ship into a conflict zone. That incident alone affected a large share of the traffic between Asia and Europe.

Corn

That brings up a good point. The repair process itself is a vulnerability. There are only about sixty to seventy specialized cable-repair ships in the entire world.

Herman

Only around sixty to seventy! For the entire planet. And many of them are old. If a major conflict broke out and multiple cables were cut simultaneously, the backlog for repairs would be years, not weeks. We are talking about a permanent or semi-permanent downgrade of the global internet.

Corn

So, when Daniel asks about the security dimensions, he is really asking about the physical security of the world's most important infrastructure. It seems like we have built this incredible digital civilization on a very thin and exposed foundation.

Herman

It is the ultimate out of sight, out of mind problem. We worry about firewalls and antivirus software, but we don't think about the fact that a single anchor in the wrong place can do more damage than a thousand hackers. And China is taking a different approach. They aren't just mapping cables; they are building their own.

Corn

You're talking about the Peace Cable, right?

Herman

Yes, the Pakistan and East Africa Connecting Europe cable. It is part of their Digital Silk Road initiative. By building and owning the infrastructure, they don't have to worry about Western tapping. They control the landing stations and the hardware. This leads to what some call the splinternet, where the physical layer of the internet is divided along geopolitical lines.

Corn

Which brings us back to the landing stations. We have talked about the cables under the sea, but they have to come ashore somewhere. Daniel mentioned the one in Denmark. Those stations must be high-value targets.

Herman

They are. A landing station is basically a small, non-descript building where the undersea cable connects to the terrestrial fiber network. If you can't tap the cable at the bottom of the ocean, you can try to compromise the landing station. This is where the light is converted into electrical signals and routed. If a government can compel the operator of a landing station to install monitoring equipment, they don't need a submarine.

Corn

And this is something that has actually happened. We know from various leaks over the years that intelligence agencies often have agreements with telecommunications companies to access data at these switching points.

Herman

Right. It is much more efficient to tap the data where it is already being processed. But this is also why there is so much tension over which companies provide the hardware for these stations. If the hardware is made by a company that is under the influence of a foreign government, there is a risk of backdoors at the most fundamental level of the network.

Corn

So, let's look at this from a practical perspective for our listeners. We have painted a pretty grim picture of giant submarines and international sabotage. But for the average person or a business, what are the takeaways?

Herman

The first takeaway is that the cloud is not a magical place in the sky. It is a physical place, and your access to it depends on these cables. If you are a business that relies on real-time data from servers in another continent, you need to understand your path diversity. Are you relying on a single cable route? If that route goes down, do you have a fallback?

Corn

And from an encryption standpoint, it sounds like we should be moving toward Quantum-Resistant encryption sooner rather than later.

Herman

Absolutely. Even if you don't think your data is being read today, you have to assume it is being recorded. Moving to post-quantum cryptography standards is the best defense we have against the store now, decrypt later threat. We also need to see more investment in cable-laying and repair capacity. It is a vital part of national security that often gets ignored because it isn't flashy.

Corn

It is like the plumbing of the world. No one thinks about it until the pipes burst and the basement is flooded.

Herman

Great analogy. And in this case, the basement is the global economy. I think what Daniel’s prompt really highlights is the paradox of our age: we are more connected than ever, but that connection is more fragile than we realize. We have traded the robustness of local systems for the efficiency of a global network, but we haven't fully accounted for the risks of that trade-off.

Corn

I wonder if we will see a move back toward more localized data storage. You know, edge computing, where the data you need is kept closer to you physically so you aren't as dependent on these international links for everything.

Herman

We are already seeing that. Companies like Amazon and Google are building massive data centers in almost every major region. They want to keep the data on-net as much as possible. But the internet is, by definition, an interconnected web. You can't truly isolate yourself without losing the very thing that makes the internet valuable.

Corn

It is a fascinating tension. The desire for a borderless digital world versus the reality of physical borders and national interests. Herman, you mentioned earlier that the cables are as thin as a garden hose. It just keeps coming back to that for me. The sheer audacity of human engineering to lay that across the Atlantic or the Pacific.

Herman

It is one of the greatest engineering feats in history. The first transatlantic telegraph cable was laid in eighteen fifty-eight. It only worked for three weeks! But it changed the world forever. Before that, a message from London to New York took ten days by ship. Suddenly, it took minutes. We have just scaled that up by a factor of billions.

Corn

And yet, here we are in January twenty twenty-six, still worried about anchors and submarines. Some things never change.

Herman

Exactly. The technology evolves, but the geography remains the same. The shortest path between two points is still a straight line, and if that line goes through a contested strait or a deep-sea trench, it is going to be a point of contention.

Corn

So, to summarize for Daniel, yes, HTTPS keeps your content private for now, but the metadata is still visible to those tapping the backbone. And the real threat isn't just someone reading your emails, it is the physical destruction of the infrastructure itself as a tool of geopolitical leverage.

Herman

Well said. It is a multi-layered security problem. You have the cyber layer, the logical layer, and the physical layer. We spend all our time on the first two, but the third one is where the real kill switch lives.

Corn

This has been such a great deep dive. No pun intended. It really makes me want to go back and look at our episode on the OSI model, episode one hundred and eighty-four, and think about that physical layer with a bit more respect.

Herman

Level one, Corn. It all starts at level one. If the photons aren't moving, nothing else matters.

Corn

Well, I think we have thoroughly explored the depths of this one. Before we wrap up, I want to say a huge thank you to Daniel for sending this in. It is exactly the kind of weird prompt that gets us thinking about the world in a different way.

Herman

Definitely. And hey, to all of you listening, if you enjoy these deep dives into the plumbing of our digital world, we would really appreciate it if you could leave us a review on Spotify or whatever podcast app you are using. It genuinely helps other curious people find the show.

Corn

It really does. You can find all our past episodes, including the ones we mentioned today, at our website, myweirdprompts dot com. We have an RSS feed there and a contact form if you want to send us your own weird prompts.

Herman

We are also on Spotify, so make sure to follow us there so you never miss an episode. We have plenty more rabbit holes to explore.

Corn

Alright, that is it for this week. I'm Corn.

Herman

And I'm Herman Poppleberry.

Corn

Thanks for listening to My Weird Prompts. We will see you in the next one.

Herman

Stay curious, everyone!

Corn

So, Herman, be honest. If you were a billionaire, would you buy a cable-repair ship or a luxury yacht?

Herman

Oh, the repair ship, no question. I’d have the most important boat in the ocean. Plus, think of the gadgets!

Corn

I knew you’d say that. I think I’ll stick to the sloth life on dry land.

Herman

Fair enough. Until next time.

Corn

See ya.

Herman

One more thing, Corn. Did you know that some of the first undersea cables were insulated with gutta-percha, which is the sap of a specific tree from Malaysia?

Corn

I did not. But I’m not surprised you did.

Herman

It was the only material that could withstand the salt water and pressure back then. We owe the internet to a tree!

Corn

A tree and some very brave sailors. Alright, let's go get some coffee.

Herman

Lead the way.

Corn

This has been My Weird Prompts. We'll be back next week with another prompt.

Herman

Can't wait. Bye for now!

Corn

Bye everyone.

Herman

Wait, did I mention the repeaters? The optical amplifiers that need high-voltage power lines running alongside the fiber?

Corn

Save it for the next one, Herman!

Herman

Right, right. Next time.

Corn

(laughs) See you then.

Herman

(fading out) It's fascinating though, thousands of volts under the ocean...

Corn

Herman!

Herman

Okay, okay, I'm coming!

Corn

(Music fades out)

Herman

(whispering) My Weird Prompts.

Corn

(whispering) Dot com.

Herman

(chuckle) Okay, now I'm done.

Corn

(final silence)