Podcast Transcript

EPISODE #284

The Ghost in the Radio: Why Number Stations Still Exist

Published January 23, 2026 • Runtime: 24:45

https://myweirdprompts.com/episode/number-stations-espionage-secrets/

EPISODE SYNOPSIS

In an era of quantum-resistant encryption and neural interfaces, the world’s most powerful intelligence agencies are still using a relic from the Cold War: the number station. This week, Herman and Corn explore the unsettling mystery of these shortwave broadcasts and the "unbreakable" mathematics of one-time pads that keep them relevant. From the physics of skywave propagation to the rise of AI-generated spy voices, discover why the most effective communication tool in 2026 is a technology nearly a century old.

DANIEL'S PROMPT

Daniel

Why are number stations still being used in 2026? If they are truly being operated by intelligence agencies, why? And what other methods might they be using as their primary form of communication?

TRANSCRIPT

Corn

Hey everyone, and welcome back to My Weird Prompts. I am Corn, and I am joined, as always, by my brother and resident expert on all things technical and obscure.

Herman

Herman Poppleberry at your service. It is great to be back in the studio, Corn. Well, I say studio, but we are really just in the living room while our housemate Daniel is probably in the kitchen wondering why we are talking about espionage at ten in the morning.

Corn

Exactly. And speaking of Daniel, he actually sent us the prompt for today's episode. He was asking about something that feels like a relic of the Cold War but is somehow still very much alive today. We are talking about number stations.

Herman

Oh, man. You are speaking my language now. Number stations are one of those things that shouldn't exist in two thousand twenty-six, right? We have quantum-resistant encryption, satellite-linked neural interfaces, and high-speed fiber everywhere. And yet, if you tune a shortwave radio to the right frequency, you will still hear a creepy, synthesized voice reading out strings of numbers in the middle of the night.

Corn

It is genuinely unsettling. I remember the first time I heard a recording of the Swedish Rhapsody or the Lincolnshire Poacher. There is something about that mechanical voice repeating five-digit blocks that just makes your skin crawl. But Daniel's question is the real kicker. Why? Why are intelligence agencies still using this in two thousand twenty-six? Is it just nostalgia, or is there a functional reason why a radio broadcast from the nineteen fifties is better than a modern encrypted app?

Herman

It is definitely not nostalgia, Corn. In the world of intelligence, if something is still being used after eighty years, it is because it is the most effective tool for the job. To understand why, we have to look at the perfect intersection of physics and mathematics.

Corn

Okay, let's start with the math. When we talk about these numbers, we are usually talking about a one-time pad, right? We have touched on this briefly in past episodes, but let's really dig into why this is considered the holy grail of secrecy.

Herman

Right. So, a one-time pad, or O T P, is the only encryption method that is mathematically proven to be unbreakable. Not just difficult to break, not just time-consuming, but literally impossible to crack, provided you follow three strict rules. First, the key must be truly random. Second, the key must be at least as long as the message itself. And third, the key must never, ever be reused.

Corn

And that is where the name comes from. You use it once, and then you destroy the pad.

Herman

Exactly. If I want to send you a message, we both have identical pads of random numbers. I use my numbers to scramble the text, and you use your identical numbers to unscramble it. To anyone else, the resulting broadcast is just white noise or a series of meaningless digits. Without that specific physical pad, there is no computer in existence, not even the most advanced quantum systems we are seeing in two thousand twenty-six, that can find a pattern, because there is no pattern to find. It is pure randomness.

Corn

That makes sense from a security standpoint, but couldn't you just send that same encrypted data over the internet? Why use a loud, public radio broadcast that anyone with a fifty-dollar receiver can hear?

Herman

That is actually the genius of it. It is what we call the hiding in plain sight principle. Think about it this way. If an operative in a foreign country is using a highly specialized, encrypted satellite phone, or even a suspicious app on their phone that pings a known C I A server, they are leaving a digital footprint. Signal intelligence agencies like the N S A or the G C H Q are looking for those spikes in traffic. They might not be able to read the message, but they know exactly who is sending it and where they are.

Corn

Right, the metadata is the giveaway.

Herman

Exactly. But a shortwave radio? A shortwave radio is a passive receiver. You don't send anything back. You just sit in your apartment, pull out a standard shortwave set, and listen. There is no way for a counter-intelligence agency to know who is listening to a broadcast that covers half a continent. You could be a spy, or you could just be a lonely hobbyist in a basement in Berlin. The act of receiving the message is completely untraceable.

Corn

That is a fascinating point. It turns the entire concept of a broadcast on its head. Usually, we think of a broadcast as something meant for everyone, but here, the fact that it is meant for everyone is the very thing that protects the one person it is actually for. It provides total anonymity for the recipient.

Herman

Precisely. And then there is the physics of shortwave radio itself, which is just cool. Shortwave uses what we call skywave propagation, or skipping. The signals bounce off the ionosphere in the upper atmosphere and curve around the horizon. This means a station in Russia, like the famous U V B seventy-six, also known as The Buzzer, can be heard thousands of miles away without needing any internet infrastructure, no satellites, and no cables.

Corn

Which makes it incredibly resilient. We talked about this a bit in episode one hundred eighty-five when we were looking at why wires still win in home networking, but this is like the ultimate version of that. If a major conflict broke out and the undersea cables were cut or the satellite constellations were jammed, these number stations would still be chirping away.

Herman

They are the ultimate backup. In fact, we have seen an uptick in number station activity recently, especially with the ongoing tensions in Eastern Europe and the South China Sea. When the digital world gets shaky, the old-school analog world becomes the bedrock.

Corn

So, we have established that they are secure and they are untraceable. But Herman, we are in two thousand twenty-six. Surely there are modern versions of this? Daniel asked what other methods agencies might be using as their primary communication. If number stations are the backup or the niche tool, what is the main event?

Herman

Well, the main event these days is often something called digital steganography. This is the art of hiding a message inside another piece of data in a way that doesn't look suspicious. Back in episode two hundred seventy-seven, we talked about A I as a shield and the art of obfuscation. Steganography is the peak of that.

Corn

Give me an example. How does that look in practice?

Herman

Imagine a high-resolution photo of a cat posted on a public social media account. To you and me, it is just a cat. But to an operative with the right software, the least significant bits of the image data have been altered to encode a message. You are talking about millions of pixels, and changing the color value of one pixel by a fraction of a percent is invisible to the human eye. It doesn't even change the file size in a way that looks weird.

Corn

So instead of a voice reading numbers over the radio, the spy is just scrolling through Instagram?

Herman

Exactly. It serves the same purpose as the number station. It is a one-to-many broadcast where the recipient remains anonymous. Millions of people look at that cat photo, but only one person knows it contains the coordinates for a dead drop.

Corn

That feels much more two thousand twenty-six. But I imagine even that has its risks. If the counter-intelligence agencies get a hold of the software used to encode the images, they can start scanning every photo on the internet.

Herman

They do. It is a constant arms race. That is why agencies are moving toward more exotic methods. There is a technique called dead drop Wi-Fi, or what some call a pirate box. An operative might install a tiny, low-power Wi-Fi router inside a hollowed-out brick or a piece of street furniture. It doesn't connect to the internet. It just sits there. When another operative walks by with a modified phone, it automatically connects and swaps data in a split second. No cell towers involved, no logs on a server.

Corn

We actually touched on the tech of covert evidence gathering in episode two hundred seventy-six, and it sounds like the same principles apply here. It is all about minimizing the window of exposure.

Herman

Right. But even with all that tech, there is a reason Daniel is still hearing about number stations. There is a simplicity to them that you just can't beat. Think about the equipment. To use a digital steganography tool, you need a computer or a smartphone. Those are inherently compromised devices. They have operating systems with backdoors, they have G P S, they have microphones. A shortwave radio from the nineteen seventies has none of that. It is a dumb device in the best possible way.

Corn

It is the ultimate air-gap.

Herman

Exactly. And let’s not forget the psychological factor. Number stations are a form of signaling. When a station like The Buzzer suddenly changes its pattern or starts reading names instead of numbers, it sends a message not just to the spies, but to the rival intelligence agencies. It says, we are here, we are active, and we are communicating. It is a bit of a cold war flex that still carries weight today.

Corn

That is an interesting angle. It is almost like a lighthouse. It is public, it is loud, and it is a constant reminder of a presence. You know, Herman, I was reading a report recently about a station called E zero six, which broadcasts in English. Apparently, they have been very active lately, and the voice sounds much more natural than it used to. It is clearly A I generated now, rather than just old-school magnetic tape loops.

Herman

Oh, definitely. They are absolutely using neural text-to-speech engines now. It is ironic, isn't it? They are using the most cutting-edge A I to generate the voice for a technology that is nearly a century old. But that actually makes it more effective. Older synthesized voices had distinct artifacts that could sometimes be used to identify the specific hardware or software used to create the broadcast. Modern A I voices are so clean and so variable that you lose that fingerprint.

Corn

So they are upgrading the old tech to make it even harder to track. That is wild.

Herman

It really is. And to Daniel’s point about why they are still being used in twenty twenty-six, we have to look at the global landscape. We are seeing a lot of countries moving toward sovereign internets, right? Russia has their Ru-Net, China has the Great Firewall, and other nations are following suit. If you are a spy in a country that has completely cut itself off from the global web, how do you get a message out? You can't use Signal. You can't use Gmail. But you can always, always hear the radio.

Corn

It is the one medium that ignores borders. You can't put a firewall in the ionosphere.

Herman

Well, you can try to jam it. We see a lot of intentional interference. But jamming is expensive, it is imprecise, and it often interferes with your own communications. It is much harder to block a shortwave signal than it is to block an I P address.

Corn

So, we have talked about the anonymity, the resilience, and the borderless nature of it. But what about the other side of Daniel’s question? If they are operated by intelligence agencies, what is the actual day-to-day use? Is it just go to this location and pick up a package, or is it more complex?

Herman

It can be anything. During the Cold War, it was often used to signal that a certain operation was a go, or to provide a new set of instructions. There is a famous story about a spy who was told to listen to a specific frequency at a specific time. If he heard a certain song, it meant he was in danger and needed to flee. Today, it is likely used for high-level coordination that needs to bypass the digital dragnet.

Corn

It is like the emergency broadcast system for the world of shadows.

Herman

That is a great way to put it. And here is something most people don't realize. Number stations aren't just for spies in the field. They are also used for diplomatic communications. If an embassy is under surveillance and they suspect their secure lines are compromised, they might fall back on a pre-arranged number station schedule to receive instructions from their home country.

Corn

Wait, really? Even embassies?

Herman

Absolutely. Specifically in high-tension zones. It is a way to ensure that the message gets through even if the local government shuts down the internet or taps the phone lines. It is the ultimate fail-safe.

Corn

I am curious about the numbers themselves. We always hear them in blocks of five. Why five? Is that a mathematical thing or just a convention?

Herman

It is mostly convention, but it has a practical purpose. Five digits is about the limit of what a human can reliably remember and write down without making a mistake. If you go to six or seven, the error rate spikes. Since these messages are often being transcribed by hand in stressful situations, you want to keep the blocks short and manageable.

Corn

That makes a lot of sense. It is the human element in an otherwise mechanical process. You know, Herman, this whole conversation reminds me of episode one hundred sixty-three, where we discussed why mainframes still run the global economy. It is that same idea that some technologies are so foundational and so reliable that replacing them with something newer actually introduces more risk than it solves.

Herman

Exactly. A mainframe is stable, it is secure, and we know exactly how it behaves. Shortwave radio is the same. We have had a hundred years to master it. We know the propagation patterns, we know the interference risks, and we know how to hide within it. When you are dealing with life-and-death intelligence work, you don't want the latest beta version of an encrypted app. You want the thing that has worked for eighty years.

Corn

So, if someone listening right now wanted to hear one of these, what would they do? I mean, obviously, we are not encouraging anyone to get involved in international espionage, but just as a curiosity.

Herman

It is actually easier than ever. You don't even need a physical radio anymore. There are these things called Web S D Rs, or Software Defined Radios, that are connected to the internet. You can go to a website, pick a radio receiver located in, say, the Netherlands or Poland, and tune it yourself from your browser. There are entire communities of hobbyists, often called radio pirates or signal hunters, who spend their time monitoring these frequencies and logging every broadcast.

Corn

And they have names for all of them, right? Like The Gong Station or The Whales.

Herman

Yes! The names are usually based on the interval signals or the specific sounds the stations make. The buzzer is the most famous because it has been broadcasting a dull, repeating drone since the late nineteen seventies. Every few years, it stops, a voice reads some names in Russian, and then it goes back to buzzing. It is one of the great mysteries of the radio world.

Corn

That is so eerie. What is the theory on that one? Is it a dead man's switch?

Herman

That is the most common theory. That it is part of a system called Perimeter, or Dead Hand. The idea is that as long as the signal is broadcasting, it means the command structure is still intact. If the signal stops, it could trigger an automated response. Of course, that is purely speculative, but it adds to the mystique.

Corn

It is amazing how much of our world is still built on these analog foundations. We think of ourselves as living in this purely digital age, but the ghosts of the twentieth century are still all around us, chirping in the background.

Herman

They really are. And I think that is the answer to Daniel's question. Number stations are still here because they solve a problem that high-tech hasn't been able to solve yet. How do you send a message to someone in total secrecy, with total anonymity, across thousands of miles, without leaving a single trace that can be followed? Until someone invents a better way to do that, the numbers will keep coming.

Corn

It is a sobering thought, actually. It means the world of espionage is just as active as it ever was, it has just gotten better at hiding.

Herman

Oh, it is more active than ever. We just don't see it because we are all looking at our screens. But the airwaves are full of secrets.

Corn

Well, on that note, let's talk about some practical takeaways for our listeners. Because while most of us aren't spies, there are things we can learn from this level of security.

Herman

Absolutely. The first big takeaway is the value of the one-time pad concept. While you probably don't need a physical pad, the principle of using a unique, random key for every interaction is the basis of modern secure communication. If you are using the same password for everything, you are essentially reusing your pad, and that is how you get cracked.

Corn

That is a great point. Diversity in your security layers is key. And another takeaway for me is the idea of the air-gap. We are so used to being constantly connected, but there is a real security benefit to having devices that aren't on the grid. If you have truly sensitive information, maybe it shouldn't be on a device with a Wi-Fi chip.

Herman

Exactly. Sometimes the best way to move forward is to take a step back into the analog world. Even something as simple as writing down your most important recovery keys on a piece of paper and putting it in a physical safe is more secure than any cloud storage.

Corn

It is the Poppleberry Method. Go low-tech when the stakes are high.

Herman

You know I love my paper notebooks, Corn. You can't hack a Leuchtturm with a remote exploit.

Corn

True. Although you can lose it on the bus, which is a different kind of security risk.

Herman

Fair point. Physical security is just as important as digital security.

Corn

Well, this has been a fascinating deep dive. Daniel, thank you for the prompt. It really opened up a rabbit hole I wasn't expecting. And to our listeners, if you have been enjoying My Weird Prompts, we would really appreciate it if you could leave us a review on your podcast app or on Spotify. It genuinely helps other people find the show and keeps us going.

Herman

It really does. We love seeing those reviews pop up. And if you want to get in touch or see the show notes for this episode, head over to my weird prompts dot com. We have got links to some of those Web S D Rs we mentioned if you want to try and find a number station yourself.

Corn

Just don't blame us if you start hearing voices in your sleep.

Herman

Hey, it is all part of the experience.

Corn

Before we wrap up, Herman, any final predictions? Do you think number stations will still be around in twenty fifty?

Herman

You know, I actually do. As long as we have an ionosphere and as long as humans have secrets, shortwave radio will have a place. It is the cockroach of communication technology. It can survive almost anything.

Corn

I love that. The cockroach of communication. Well, that is a wrap for episode two hundred eighty. Thank you all for listening to My Weird Prompts. I am Corn.

Herman

And I am Herman Poppleberry.

Corn

We will see you next week, where we might just be diving into something a little less shadowy, but hopefully just as weird.

Herman

Until then, keep your ears open and your pads secret.

Corn

Stay curious, everyone.

Herman

Bye now!

Corn

Take care.

Herman

Oh, and Corn?

Corn

Yeah?

Herman

I think I heard a series of beeps coming from your toaster this morning. You might want to check if it is transmitting to a submarine in the Mediterranean.

Corn

Very funny, Herman. It was just the bagel setting.

Herman

That is exactly what a spy would say.

Corn

Goodbye, Herman.

Herman

Goodbye!