Podcast Transcript

EPISODE #223

Beyond the Blackout: Tech for Digital Survival

Published January 13, 2026 • Runtime: 25:08

https://myweirdprompts.com/episode/digital-survival-internet-censorship/

EPISODE SYNOPSIS

How do you stay connected when a regime tries to "vanish" the internet? In this episode of My Weird Prompts, Herman and Corn dive deep into the mechanics of digital isolation, moving beyond the headlines to examine the high-stakes game of cat and mouse between state censors and activists. From the surgical manipulation of Border Gateway Protocol (BGP) to the surprising physical vulnerabilities of satellite internet, the brothers explore why "unblockable" technology is often a myth. They also highlight the "low-and-slow" innovations keeping information flowing in conflict zones, including LoRa mesh networks, the Snowflake protocol, and the enduring power of the physical "sneakernet." It is a fascinating look at asymmetrical digital warfare and the resilient tools designed to punch holes in the world’s most sophisticated firewalls.

DANIEL'S PROMPT

Daniel

We recently discussed BGP (Border Gateway Protocol) and the mechanics of the internet, specifically how it serves as a choke point for regimes like the IRGC in Iran to monitor traffic and restrict connectivity. We previously talked about satellite internet, such as Starlink, as a "last hope" for dissidents and journalists, but the Iranian regime has now started jamming Starlink signals. This is concerning as LEO satellites were thought to be more resilient. Additionally, satellite uplinks are high-risk because they leave a conspicuous RF signature that makes it easier for the regime to localize users. What can people do in the most challenging connectivity environments to get packets out and tell their stories to the outside world?

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.

Herman

Herman Poppleberry, reporting for duty. And it is a beautiful, if slightly chilly, morning here.

Corn

It really is. Our housemate Daniel sent us a voice memo this morning that actually hits on a topic we have been circling for a while. It is about the mechanics of staying connected when the world around you is trying to pull the plug. Specifically, he was asking about how people in high-pressure environments, like what we see with the chronic internet restrictions in places like Iran, can actually get information out when the standard tools start to fail.

Herman

This is such a critical topic. Daniel mentioned the Border Gateway Protocol, or BGP, which we took a deep dive into back in episode one hundred and eighty-seven. For those who missed that one, BGP is essentially the glue of the internet. It is how different networks decide the best path for data to travel. But as Daniel pointed out, that same glue can be used to create a choke point. If a regime controls the BGP tables, they can effectively vanish parts of the internet or reroute your traffic through a surveillance middleman.

Corn

Right, and the conversation has shifted lately. For a long time, the narrative was that satellite internet, specifically Low Earth Orbit constellations like Starlink, was the ultimate workaround. The idea was that you cannot stop a signal coming from space. But Daniel mentioned something concerning: the reality of jamming and the risk of radio frequency signatures.

Herman

Exactly. There is this myth of the unblockable technology. People think that because a satellite is five hundred kilometers up in space, it is untouchable. But the physics of radio tells a different story. If you are sitting in a city and you have a satellite dish on your roof, you are still communicating on specific frequencies. If a government wants to stop that, they do not need to go to space. They just need to make more noise on the ground than the satellite is making from orbit.

Corn

I want to dig into that jamming aspect in a minute, but first, let's set the stage for why this is so difficult. When we talk about these challenging connectivity environments, we are not just talking about a slow website. We are talking about total digital isolation. Herman, you have been looking into how the Border Gateway Protocol is being manipulated these days. Is it getting more sophisticated?

Herman

It really is, Corn. In the past, a government might just shut off the power to a data center or cut a fiber optic cable. That is a blunt instrument. It works, but it also kills the economy. What we are seeing now is much more surgical. By manipulating BGP advertisements, a state-controlled Internet Service Provider can tell the rest of the world that they are the best path for traffic destined for, say, a secure messaging app.

Corn

So, instead of blocking the app, they just tell the internet to send all the messages to their servers first?

Herman

Precisely. It is a massive man-in-the-middle attack at the scale of a whole nation. They can inspect the metadata, identify who is talking to whom, and then either drop the packets or pass them along after they have logged everything. This is why BGP is such a powerful tool for censorship. It happens at the routing layer, which is invisible to most users. Your phone says you are connected, but your data is taking a very dangerous detour.

Corn

That is terrifying because it bypasses the basic assumption that if you have a signal, you are safe. But let's talk about the satellite workaround. Daniel mentioned that while we used to see Starlink as this resilient last hope, the reality is more complicated. Why is jamming so effective against something as advanced as a Low Earth Orbit satellite?

Herman

It comes down to the signal-to-noise ratio. Think of it like trying to have a conversation in a library versus a rock concert. The satellite is the person whispering to you from across the room. It is very far away, and its signal is relatively weak by the time it reaches your dish. Now imagine the government pulls up a van outside your house with a massive speaker and just starts blasting static. That is jamming.

Corn

So, it does not matter how smart the satellite is if the receiver on the ground is drowned out by local noise.

Herman

Exactly. And while Starlink uses phased array antennas that can null out interference from certain directions, it is not perfect. If you have multiple jammers or a high-powered transmitter nearby, the receiver just gets overwhelmed. There have been reports of this happening in various conflict zones and high-surveillance areas. It is a game of cat and mouse. The satellite tries to hop frequencies, and the jammer tries to cover the whole spectrum.

Corn

And then there is the other side of the coin that Daniel brought up: the radio frequency signature. This is something I think a lot of people overlook. Even if your satellite link is working perfectly, you are still a lighthouse in a dark room.

Herman

That is a great analogy, Corn. Every time your dish sends a packet up to the satellite, it is emitting a high-frequency radio signal. To a government with direction-finding equipment, that signal is a beacon. They do not even need to know what you are saying. They just need to see that there is a high-bandwidth uplink coming from a specific rooftop in a specific neighborhood.

Corn

So, they can triangulate your exact position just from the radio waves?

Herman

Within meters. We are talking about sophisticated electronic warfare tools that can be mounted on a truck or even a drone. If you are a journalist or an activist using a satellite uplink in a hostile city, you are essentially painting a target on your roof. This is the big trade-off. Satellite gives you a path out, but it also makes you very easy to find.

Corn

This brings us to the core of Daniel's question. If BGP is compromised and satellites are both jammable and dangerous to use, what are the alternatives? How do you actually get a story out when the traditional paths are closed?

Herman

This is where we have to look at what I call the low-and-slow approach. If you cannot use a high-powered satellite dish, you have to look at things that blend into the background noise. One of the most fascinating developments is the use of mesh networking and low-power radio protocols.

Corn

Like LoRa? I know we have talked about that in passing before.

Herman

Yes, LoRa, which stands for Long Range. It is a protocol designed for the Internet of Things, like sensors and smart meters. It uses very little power and sends data very slowly, but it can travel kilometers. Because the power is so low, it is much harder for direction-finding equipment to pick it up. It often sits below the noise floor of standard radio equipment.

Corn

So, instead of a lighthouse, it is more like someone clicking a flashlight very faintly?

Herman

Exactly. And if you have a hundred people with these little devices, they can form a mesh. If I want to send a message but I am not near a gateway, my device sends it to yours, yours sends it to the next person, and eventually, it finds a way out. There is a protocol called Reticulum that is designed exactly for this. It is a cryptography-first networking stack that can run over anything: radio, wifi, even a piece of paper with a QR code if you are desperate enough.

Corn

Wait, a piece of paper? How does that work in a digital network?

Herman

It is about the abstraction. Reticulum does not care what the physical medium is. You can encode a packet into a QR code, someone carries that code across a border, and then it is scanned and re-injected into the network. It is the ultimate evolution of the sneakernet.

Corn

The sneakernet. That is a classic. For the younger listeners, that is just the idea of physically carrying data on a disk or a thumb drive. It sounds ancient, but in a total blackout, it is actually the highest bandwidth connection you can have.

Herman

It really is. Never underestimate the bandwidth of a station wagon full of hard drives moving at sixty miles per hour. Or in a modern context, a micro SD card sewn into the lining of a jacket. A single one-terabyte micro SD card can hold more information than a month of satellite uplinks. If you are trying to get raw video footage of an event out of a country, sometimes the safest and fastest way is to give that card to someone who is taking a bus across the border.

Corn

But that has its own risks, obviously. Physical searches, checkpoints. I am curious about the middle ground. What about when the internet is still on, but it is heavily filtered? We have talked about VPNs a million times, but Daniel mentioned that they are becoming less effective because regimes are getting better at identifying VPN traffic.

Herman

Right. Standard VPN protocols like OpenVPN or WireGuard have very specific signatures. They are easy for a Great Firewall to spot and throttle. This is why we are seeing a shift toward obfuscation. Have you looked into the Snowflake project from Tor?

Corn

I have heard the name. It is a pluggable transport, right?

Herman

Yes. The brilliance of Snowflake is that it makes your internet traffic look like something completely mundane, like a WebRTC video call. When you use Snowflake, you are not connecting to a known Tor bridge. Instead, you are connecting to a regular person's browser somewhere in the world. That person has a little extension installed that acts as a temporary bridge. To the government's filters, it just looks like you are having a random video chat with someone in Germany or Canada.

Corn

That is clever because they cannot block all video calls without breaking the whole internet for everyone. It is that idea of hiding in plain sight.

Herman

Exactly. And the numbers on this are staggering. During periods of intense censorship in various regions over the last few years, we have seen the number of Snowflake bridges scale up to meet the demand. It is a decentralized, volunteer-driven way to punch holes in a firewall. But even that requires a basic internet connection. If the fiber is cut and the cell towers are down, Snowflake cannot help you.

Corn

So, we are back to the physical reality. If the grid goes dark, you need your own infrastructure. I was reading about people using amateur radio, like packet radio, to send emails. Is that still a viable thing?

Herman

It is, though it is a very niche skill. Amateur radio operators have been doing this for decades. There is a system called Winlink which allows you to send emails over high-frequency radio bands. These signals can bounce off the ionosphere and travel thousands of kilometers, completely bypassing local infrastructure. You could be in the middle of a blackout in one country and be sending an email to a server in a different continent.

Corn

But again, the radio frequency signature. An amateur radio transmitter is not exactly subtle.

Herman

No, it is definitely not. If you are using a big antenna and a hundred watts of power, you are very visible. This is why the focus for dissidents is shifting toward these low-power mesh networks. You want something that looks like background noise. You want to be one of ten thousand low-power devices in a city rather than the one guy with a massive antenna on his roof.

Corn

It is about changing the math for the censor. If it costs them a million dollars in equipment and ten hours of man-power to find one person sending a tiny text message, the system eventually breaks down. They cannot find everyone.

Herman

That is the goal of a lot of these projects. It is about asymmetrical digital warfare. You want to make the cost of censorship higher than the cost of the technology used to bypass it.

Corn

I want to go back to something Daniel mentioned about the "stealth" aspect of antennas. He was asking if there are ways to hide the physical presence of something like a Starlink dish or a radio antenna. I have seen people talking about disguising them as air conditioning units or hiding them inside plastic containers that do not block radio waves. Is that a real strategy?

Herman

It is a very real strategy. In the world of radio, we call these materials radomes. Basically, any material that is transparent to radio waves. Certain types of plastic, fiberglass, or even treated wood can be used to hide an antenna. You could have a high-gain antenna inside a fake plastic planter on your balcony, and to a drone flying over, it just looks like a dead fern.

Corn

But the heat signature might still be an issue, right? Electronics get warm.

Herman

That is a very sharp observation, Corn. Sophisticated surveillance can use thermal imaging. A Starlink dish, for example, consumes a fair amount of power and has a very distinct thermal footprint. If you are in a cold environment, that dish is going to glow like a lightbulb on an infrared camera. So, you have to think about thermal shielding and ventilation too. It is never just one thing. It is a whole stack of physical and digital security.

Corn

It feels like we are describing a world where you have to be a radio engineer, a computer scientist, and a master of disguise just to send a tweet. It is a lot to ask of a regular person who just wants the world to know what is happening in their street.

Herman

It is a huge burden. And that is why the most important work being done right now is in making these tools easier to use. We need "one-click" solutions for things like Reticulum or Snowflake. If it is too hard to set up, people will not use it, or they will make a mistake that gets them caught.

Corn

Let's talk about the practical takeaways. If someone finds themselves in a situation where the internet is failing, what are the tiers of action? Like, what is the first thing you do, and what is the last resort?

Herman

Tier one is always preparation. Before the lights go out, you need to have your tools ready. That means downloading a variety of VPNs, but also more resilient tools like the Tor Browser and the Snowflake extension. You should also have offline maps and communication apps that work over local wifi or bluetooth, like Briar.

Corn

Briar is great because it does not need a server at all. If you and I are in the same building, our phones can talk to each other directly.

Herman

Exactly. Tier two is obfuscation. If the government starts blocking VPNs, you move to pluggable transports. You try to make your traffic look like something else. This is where Snowflake and ShadowSocks come in. You are trying to stay on the grid but stay invisible.

Corn

And Tier three?

Herman

Tier three is when the grid is gone. This is where you move to the physical and the alternative. This is the sneakernet. It is the micro SD cards. It is the mesh networks. If you have a LoRa device and a friend ten kilometers away has one, you have a private link that no one can shut off by flipping a switch at an Internet Service Provider.

Corn

And Tier four is the high-risk stuff, right? The satellites and the long-range radio.

Herman

Right. That is the last resort because of the visibility. You only use those if the information you have is so important that it is worth the risk of being located. And if you do use them, you use them for the shortest time possible. You turn it on, burst your data, and turn it off. You do not stay connected for hours. You are a ghost.

Corn

It is amazing to think about the evolution of this. We went from the early days of the internet, which was built to be decentralized and resilient, to a very centralized system where a few BGP entries can silence a nation, and now we are looping back to these decentralized, almost "primitive" radio methods to reclaim that resilience.

Herman

It is a cycle. The internet grew up and got corporate and centralized because it was efficient. But efficiency is the enemy of resilience. When you have a central point of failure, a censor only has to stand in one place to block everything. By going back to mesh networks and point-to-point radio, we are rebuilding the internet the way it was originally envisioned: a web that can route around damage.

Corn

Even if that damage is a government filter. Herman, you mentioned Reticulum earlier. I want to go a bit deeper on that. How does it actually handle the "addressing" problem? If there is no central server, how do I find you in a mesh?

Herman

That is the beauty of it. Reticulum uses what is called an identity-based addressing system. My address is essentially a cryptographic public key. When I send a message into the mesh, the network does not need a map of where everyone is. It just needs to know how to move that packet one step closer to someone who has seen my key recently. It uses a very efficient routing algorithm that works even on very slow links.

Corn

So, it is like word-of-mouth for data?

Herman

Exactly. "Hey, have you seen Herman?" "No, but I know a guy who was talking to him ten minutes ago. Give me the packet, and I will pass it that way." It is incredibly robust. And because everything is encrypted by default, even if someone intercepts the packet in the middle of the mesh, they cannot see what is inside or even who it is ultimately for until it reaches the destination.

Corn

That feels like a huge leap forward for privacy in these environments. But what about the latency? If I am sending a message through ten different people's LoRa devices, it is not going to be instant, is it?

Herman

Oh, absolutely not. We are talking about seconds or even minutes for a simple text message. This is not for scrolling through social media. This is for critical communication. It is for saying "I am safe," or "The protest is moving to the main square," or "Here is a link to a file I just hid in a dead drop." It is about getting the essential packets out.

Corn

I like that distinction. We are so used to the "always-on, high-speed" internet that we forget how much can be accomplished with just a few kilobytes of data if it is the right data.

Herman

There is a project called the Global Mesh Labs that is working on exactly this. They are trying to create a sustainable, long-range mesh network that can be used for everything from emergency services to resisting censorship. They are even looking at how to integrate lightning payments over these mesh networks so people can buy and sell things without a central bank.

Corn

Now that is a second-order effect I had not considered. If the internet goes down, the economy usually goes with it because no one can process payments. If you can run a basic financial system over a mesh network, you have a level of resilience that is almost impossible to break.

Herman

It is the ultimate "dark net," not in the sense of illegal activity, but in the sense of a network that exists in the shadows of the formal infrastructure. It is a parallel world.

Corn

So, to bring it back to Daniel's question about the IRGC and the situation in Iran. The reality is that while the regime is getting better at jamming and monitoring BGP, the toolkit for the individual is also expanding. It is a constant arms race.

Herman

It really is. And the most important thing for people outside these zones is to keep providing the "exit points." A mesh network in Tehran is only useful if someone, somewhere, can bridge it to the global internet. This is why things like Snowflake are so vital. We are providing the "other side" of the bridge.

Corn

It makes me think about our own responsibility. We often take our fiber connections for granted here in Jerusalem, but we are only a few hops away from these more restricted networks.

Herman

Exactly. We are all part of the same BGP table, after all.

Corn

That is a great place to start wrapping up this part of the discussion. We have covered a lot of ground: from the high-level routing of BGP to the physical risks of satellite uplinks, and the emerging world of low-power mesh networks. It is a complex landscape, but the underlying theme is clear: where there is a will to communicate, people will find a way, even if they have to reinvent the radio to do it.

Herman

And I think that is the most inspiring part. The technology is just a tool. The real resilience comes from the people who are willing to take these risks to tell their stories. Whether it is sewing an SD card into a jacket or setting up a LoRa node in a window, it is that human drive to stay connected that ultimately wins.

Corn

Well said, Herman. We should probably mention that if you want to dig deeper into any of these specific protocols, we have links and more detailed breakdowns on our website at myweirdprompts.com. We have also got a contact form there if you have your own "weird prompt" you want us to tackle. We have been doing this for over two hundred episodes now, with many more in the archives, and it is the feedback from listeners that keeps us diving into these rabbit holes. So, thank you to Daniel for the prompt today. It definitely kept us on our toes.

Herman

It certainly did. I think I am going to go check on our own mesh setup now, just in case.

Corn

Good idea. Alright everyone, thanks for listening to My Weird Prompts. I am Corn.

Herman

And I am Herman Poppleberry. We will catch you in the next one.

Corn

Stay curious, and stay connected. Bye for now.

Herman

Bye!