Podcast Transcript

EPISODE #209

The Digital Kill Switch: BGP, DPI, and Satellite Rebels

Published January 09, 2026 • Runtime: 25:39

https://myweirdprompts.com/episode/internet-shutdowns-satellite-bypass/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, hosts Herman and Corn explore the technical architecture behind state-sponsored internet shutdowns and the emerging technologies designed to bypass them. They analyze how governments utilize Border Gateway Protocol (BGP) withdrawals and Deep Packet Inspection (DPI) to isolate citizens, while also examining the rise of "Sovereign Internets" like Iran's National Information Network. The conversation then looks upward to the stars, detailing how Low Earth Orbit satellite constellations and new direct-to-cell capabilities are rendering traditional digital borders porous. By contrasting the physical geography of terrestrial cables with the borderless potential of space-based data, the duo provides a comprehensive overview of the modern battle for information freedom in 2026.

DANIEL'S PROMPT

Daniel

"I'd like to discuss internet connectivity and how it works at the network level, particularly in the context of governments cutting off access during periods of unrest. How do regimes practically block or choke internet entry and exit points? Additionally, how can individuals like dissidents or journalists find ways to maintain connectivity or get messages out—perhaps through satellite or low earth orbit (LEO) networks—when the terrestrial internet is blocked?"

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. It is January ninth, twenty twenty-six, and we are diving into a topic that feels particularly heavy and urgent right now. I am Corn, and sitting across from me in our Jerusalem living room is my brother.

Herman

Herman Poppleberry, ready to get into the weeds. And yeah, Corn, this is a big one. Our housemate Daniel sent us a prompt after following the news out of Iran. There have been repeated waves of massive protests in recent years—often intensified by economic crises and currency shocks—and as we saw during those extended internet disruptions back in mid-twenty twenty-five, the government has repeatedly been clamping down on the digital gateways.

Corn

It is a pattern we see over and over again, right? When things get tense on the ground, the digital lights go out. Daniel was asking about the actual mechanics of this. How do you even turn off the internet for an entire country? And more importantly, if you are a journalist or a dissident on the ground, how do you get a message out when the terrestrial lines are cut?

Herman

It is a fascinating and terrifying intersection of networking protocol and state power. We have talked about the internet in a lot of different contexts. I think back to episode one hundred eighty-four when we did that deep dive into the Open Systems Interconnection model, the OSI model. But today we are looking at the internet not as an abstract stack of layers, but as a physical and political geography that can be manipulated.

Corn

Exactly. It is not just magic in the air. It is cables, routers, and very specific protocols that govern how data moves across borders. So, Herman, let us start with the basics of that geography. When we talk about a country like Iran or any nation state, how is their internal network actually connected to the rest of the world?

Herman

To understand how you kill the internet, you have to understand what holds it together. The internet is essentially a network of networks. We call these Autonomous Systems. Think of an Autonomous System as a giant neighborhood managed by a single entity, like an Internet Service Provider or a large university. Right now, there are on the order of seventy-five to eighty thousand of these Autonomous Systems globally.

Corn

And they all have to talk to each other to move data from, say, a server in California to a phone in Tehran.

Herman

Precisely. And the language they use is called Border Gateway Protocol, or BGP. This is the glue. BGP is how these Autonomous Systems tell each other which IP addresses they can reach. It is like a global map that is constantly being updated. If I am an Internet Service Provider in Turkey, I tell my neighbors, hey, if you want to reach these specific Iranian addresses, send the data through me.

Corn

So, if a government wants to cut off the outside world, do they just tell their domestic Internet Service Providers to stop talking Border Gateway Protocol to the neighbors?

Herman

That is the most blunt way to do it. It is called a BGP route withdrawal. The government orders the state-owned or state-controlled Internet Service Providers to stop announcing their routes to the global internet. Suddenly, to the rest of the world, those IP addresses simply cease to exist. The data has no map to get there, so it just drops. We have seen this play out in multiple past crises, where connectivity in countries like Iran dropped to just a tiny fraction of normal levels within hours.

Corn

But that seems like an all-or-nothing move. If you do a full BGP withdrawal, you are killing your own economy too, right? Banks can not process transactions, government offices can not communicate. It is a digital scorched earth policy.

Herman

You are spot on. And that is why we have seen a shift in how sophisticated regimes handle this. They have spent the last decade building what people call the Splinternet or a Sovereign Internet. In Iran, they call it the National Information Network, or the NIN.

Corn

I remember reading about this. The idea is to create a domestic version of the internet that can function even if the umbilical cord to the global web is severed.

Herman

Exactly. They want to have their cake and eat it too. They host domestic versions of messaging apps like Soroush, banking services, and government portals on local servers within the country. Then, when unrest hits, they can throttle or completely block the international gateways while keeping the local network humming. It allows the state to continue functioning while the citizens are cut off from international news and social media. It is what analysts are calling 'measured disruption'—keeping the economy on life support while silencing the streets.

Corn

So it is less like a single kill switch and more like a series of valves they can turn.

Herman

Exactly. They use something called Deep Packet Inspection, or DPI. This is where it gets really granular. Instead of just blocking everything, they have these powerful middleboxes at the border. These boxes look at the actual data packets as they fly by. They can see, oh, this packet is encrypted using a protocol common to Virtual Private Networks, or this packet is headed for a known WhatsApp server. They can then choose to drop those specific packets or, even more effectively, choke the bandwidth so much that the service becomes unusable.

Corn

That choking or throttling seems almost more insidious than a total blackout. If it is just really slow, people might think it is a technical glitch rather than a deliberate act of censorship. It creates this sense of frustration and isolation without the clear evidence of a total shutdown.

Herman

It is a classic psychological tactic. If you can only send one text every ten minutes, you can not coordinate a protest in real time. You can not upload a video of police brutality to Twitter or YouTube because the upload will just time out. It breaks the real-time nature of the modern web.

Corn

We have talked about the vulnerabilities of the internet before, like in episode one hundred seventy-three when we discussed achieving the gold standard of uptime. But there, we were talking about accidental failures. Here, the failure is the feature. So, if you are Daniel's hypothetical dissident or journalist, and you are sitting in a city where the terrestrial fiber has been throttled or BGP routes have been withdrawn, what are your options?

Herman

This is where the technology has really shifted in the last few years, especially as we move into twenty twenty-six. Historically, your options were very limited. You might try a dial-up modem to an international number if the phone lines were still open, but that is incredibly slow and easy to track. You might use a mesh network with your neighbors, but that only helps you talk to people within a few hundred meters.

Corn

But now we have the sky.

Herman

We have the sky. Low Earth Orbit satellite constellations have completely changed the game. Most people are familiar with Starlink, which now has over five thousand satellites in orbit. But we also have Amazon's project, called Project Kuiper. In late twenty twenty-five they began early testing of their satellites and announced plans to start limited customer trials as they ramp up service over the next couple of years.

Corn

Right, and these Low Earth Orbit satellites are only a few hundred kilometers up, unlike the old geostationary ones.

Herman

Exactly. Because they are so close, the latency is low enough for video calls. But the real magic for a dissident is that these satellites bypass the domestic terrestrial infrastructure entirely. When your terminal talks to a satellite, that signal goes up to space, and then it is passed between satellites using laser links until it reaches a ground station thousands of miles away in a friendly country.

Corn

So the Iranian government, or any government, has no way to intercept that data because it never touches an Iranian router.

Herman

Precisely. It circumvents the entire national gateway. No Deep Packet Inspection, no BGP withdrawal, no throttling. As long as you have a clear view of the sky and a terminal, you are on the global internet.

Corn

But there is a massive catch here, isn't there? You need the hardware. You can't just download an app to connect to a satellite. You need a dish, or at least a specialized antenna. How do you get that into a country where the government is actively looking for it?

Herman

That is the physical challenge. These terminals are small—the Starlink Mini is about the size of a laptop—but they still have to be smuggled in. We have seen reports of terminals being smuggled into tightly controlled countries in the back of trucks or hidden in shipments of other electronics. It is a high-stakes game of cat and mouse.

Corn

And once you have the terminal, aren't you a target? I mean, the government can probably see that there is a satellite signal coming from a specific house.

Herman

That is a very real risk. Radio frequency detection is a thing. If the government has the right equipment, they can triangulate where a satellite uplink is coming from. It is not as easy as finding a radio station, because the beam from a satellite dish is very narrow and pointed up, but it is not impossible. Users have to be very careful, maybe only turning the device on for short bursts or camouflaging the dish.

Corn

It reminds me of the old days of shortwave radio, where people would huddle around a receiver to hear news from the outside world, except now they are huddling around a Wi-Fi router connected to a piece of space tech.

Herman

It really is the modern equivalent. But here is where it gets even more interesting, Corn. We are starting to see the rise of direct-to-cell satellite technology. This is something that was just a dream a few years ago, but here in early twenty twenty-six, it is moving from experiment to early trials.

Corn

Wait, you mean my regular smartphone can talk to a satellite without a pizza box dish?

Herman

Yes. SpaceX and T-Mobile, along with AST SpaceMobile, have been launching satellites with massive antennas—some on the order of several hundred square feet, like AST's BlueWalker 3 test satellite—that can pick up the signals from a standard unmodified smartphone. As of this month, we are seeing the first test deployments and early trial services in places like the United States and Ukraine, with wider commercial rollouts expected over the next couple of years.

Corn

That is a game changer for a journalist in a protest. You don't need to smuggle in a dish. You just need the phone you already have in your pocket.

Herman

It is the ultimate nightmare for a repressive regime. How do you block a signal that is coming from hundreds of miles straight up, hitting every phone in the city? You can't really jam the entire satellite frequency without also disrupting your own military and commercial communications. It makes the digital iron curtain incredibly porous.

Corn

But I assume the governments aren't just giving up. If they can't block the signal, they go after the people.

Herman

Absolutely. The battle moves from the network layer to the physical and legal layers. They might pass laws making it a severe crime to possess a satellite terminal. They might use social engineering or malware to infect the phones and see who is using these services. It becomes a war of attrition.

Corn

I want to go back to the network level for a second. You mentioned BGP earlier. Is there any way for a government to use BGP to actually hijack traffic rather than just blocking it?

Herman

Oh, absolutely. This is called BGP hijacking, and it is a major security flaw in how the internet was designed. Because BGP relies on trust, an Autonomous System can essentially lie. It can say, hey, I am the fastest route to Google's servers. If other routers believe that lie, they will start sending Google-bound traffic to that dishonest network. We have seen versions of this before, such as past BGP leaks involving Orange Spain in Europe and separate incidents involving Tata Communications in India.

Corn

And once the government has that traffic, they can inspect it, modify it, or just drop it.

Herman

Exactly. A state-owned ISP can announce that it owns the IP space for a popular encrypted messaging app. For a few hours, all the messages intended for that app might flow through the government's servers before being passed along. If the encryption is strong, they might not be able to read the messages, but they can see who is talking to whom, which is often enough to start making arrests.

Corn

It is that metadata again. Even if you have the lock, they can see who you are sending the key to.

Herman

Exactly. And this is why we always tell people that tools like Tor or very high-quality VPNs are essential, but even they have limits during a total network shutdown. A VPN needs a path to its server. If the government has blocked all international traffic at the BGP level, your VPN has nowhere to go.

Corn

So, in a total shutdown, the only real exit is up.

Herman

Pretty much. Either up to a satellite or physically carrying a hard drive across a border. It is a return to what people call sneakernet, where you literally put data on a physical device and move it.

Corn

It is amazing to think that in twenty twenty-six, with all our fiber optics and five G, we might still rely on someone carrying a thumb drive across a mountain pass.

Herman

It shows that the physical world still matters. The internet feels like this ethereal, omnipresent thing, but it is tethered to the ground. It is tethered to the laws of the countries it passes through.

Corn

You know, we should probably talk about the role of international companies in this. When a government like Iran's orders a shutdown, are the private ISPs just following orders, or do they have a choice?

Herman

In most of these countries, the ISPs are either state-owned or they operate under very strict licenses that require them to comply with national security orders. If they don't flip the switch, the government can just send in the police to pull the plugs physically. There isn't much room for corporate civil disobedience when the state has a monopoly on violence.

Corn

It is a stark reminder of the power of the state. We often think of the internet as this decentralized, uncontrollable force, but at the border, it is very centralized.

Herman

That is the core of the problem. We designed the internet to be resilient against technical failure, but we didn't necessarily design it to be resilient against state-level malice at the gateway points.

Corn

So, what is the long-term solution? Is it just more satellites?

Herman

Satellites are a huge part of it. But there is also a movement toward more decentralized web protocols. Things like IPFS, the InterPlanetary File System, or various blockchain-based naming systems. The goal is to make it so there is no single point of failure or control. If the data is distributed across thousands of peer-to-peer nodes, it becomes much harder to kill.

Corn

But even those need a physical network to run on. You still need those packets to move from point A to point B.

Herman

Exactly. You can have the most decentralized software in the world, but if the government cuts the fiber optic cable, the software has nothing to talk to. That is why the combination of decentralized software and decentralized hardware, like LEO satellites and mesh networks, is the real frontier for internet freedom.

Corn

It is a fascinating arms race. The governments build better filters, the dissidents find better tunnels. The governments cut the cables, the dissidents look to the stars.

Herman

And it is not just happening in Iran. We see versions of this in many places. The technology of control is being exported. There is a whole industry of companies that sell Deep Packet Inspection and surveillance gear to these regimes.

Corn

That is the dark side of the tech industry. The same tools we use to manage corporate networks and keep them safe are being repurposed to silence entire populations.

Herman

It is the dual-use nature of technology. A firewall can keep a hacker out, or it can keep a citizen in.

Corn

Herman, you mentioned earlier that some countries are building their own sovereign internets. How close is that to becoming a reality? Could we actually see a world where the internet isn't one global network anymore, but a series of interconnected but separate national networks?

Herman

We are already there, Corn. Some people call it the Splinternet. China's Great Firewall is the most famous example, but Russia has been testing its RuNet for years, and Iran has its National Information Network. They are essentially creating their own digital islands. They have their own DNS, their own root servers, their own versions of every major service. They can still talk to the outside world if they want to, but they don't need to.

Corn

That feels like a massive step backward for humanity. The whole promise of the internet was that it would connect us all, regardless of borders.

Herman

It is a tragic irony. The more we connect, the more some people want to build walls. But as we have seen, those walls are never perfect. There is always a crack, whether it is a satellite signal, a smuggled terminal, or a clever new encryption protocol.

Corn

It makes me think about what we discussed in episode one hundred fifty-one about why your gigabit internet might feel slow. We were talking about domestic mesh versus wired setups. But on a national scale, that mesh could be the difference between information and total silence.

Herman

Absolutely. Imagine a city where every balcony has a small, low-power mesh node. Even if the main internet goes down, the city can still talk to itself. People can share news, coordinate medical help, and pass information toward the few people who might have a working satellite link. It is about building layers of redundancy.

Corn

It is that old engineering principle. Don't rely on one path.

Herman

Exactly. And for the listeners out there who are lucky enough to live in places where the internet is open, it is easy to take this for granted. But understanding these mechanisms is the first step toward protecting them.

Corn

Well, I think we have covered a lot of ground, or rather, a lot of space. We went from BGP route withdrawals to Deep Packet Inspection and then up to the Low Earth Orbit satellites that are providing a lifeline to people in places like Iran.

Herman

It is a lot to digest. But the takeaway for me is that while the state has immense power over the physical infrastructure, the human desire for connection and information is incredibly resourceful. We are seeing the early stages of a truly global, harder-to-block internet, even if it is currently a very expensive and difficult birth.

Corn

It is a hopeful note in a pretty dark topic. Daniel, thank you for sending that in. It is a question that really forced us to look at the plumbing of the world in a way we don't usually do.

Herman

Yeah, it is easy to stay at the application layer where everything is just icons on a screen. But the real battle is happening at the routing layer and in the vacuum of space.

Corn

Before we wrap up, I want to remind everyone that if you are enjoying these deep dives, please take a moment to leave us a review on your podcast app or on Spotify. It really does help the show reach more curious people like you.

Herman

It genuinely makes a difference. And if you want to get in touch or see our back catalog, head over to myweirdprompts.com. We have all two hundred and nine episodes there, and a contact form if you have a weird prompt of your own.

Corn

We are always looking for new rabbit holes to dive into. Herman, any final thoughts on the future of the Splinternet?

Herman

I think twenty twenty-six and twenty twenty-seven will be the years where we see whether the satellite revolution can truly start to break the back of digital censorship. It is a high-stakes experiment happening right over our heads every single day.

Corn

Well, we will be watching. Thanks for listening to My Weird Prompts. I am Corn.

Herman

And I am Herman Poppleberry. We will catch you next time.

Corn

Stay curious, everyone.

Herman

And keep looking up.

Corn

Exactly. The answers are usually up there somewhere.

Herman

Alright, let us go see if Daniel has any more coffee. I think we earned it after that one.

Corn

Good idea. See you later, everyone.

Herman

Bye!

Corn

You know, I was just thinking about that laser link technology you mentioned. How does a satellite actually aim a laser at another satellite while they are both moving at seventeen thousand miles an hour?

Herman

Oh, Corn, that is a whole other episode. The precision required is insane. It is like trying to hit a moving penny with a laser pointer from five miles away while you are on a roller coaster. We should definitely put that on the list for future topics.

Corn

Added. The physics of satellite lasers. That sounds like a Herman special.

Herman

Guilty as charged. I will start reading up on it tonight.

Corn

I figured you would. Alright, let us wrap this for real. Thanks again for tuning in. This has been My Weird Prompts.

Herman

Take care, everyone!