Podcast Transcript

EPISODE #370

Bunkers and Bytes: The Secret World of Gov Clouds

Published January 30, 2026 • Runtime: 25:41

https://myweirdprompts.com/episode/top-secret-cloud-infrastructure/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, Herman and Corn dive into the complex intersection of commercial cloud giants and the global intelligence community. They explore how companies like Amazon and Microsoft have moved from hosting public websites to managing the world's most sensitive intelligence data. From the CIA’s landmark 2013 deal with AWS to the rise of sovereign clouds and air-gapped data centers, the brothers break down the engineering marvels that make this possible. Discover the reality of data diodes, SCIFs, and the multi-billion dollar shift toward a cloud-based national security apparatus where the most advanced AI in the world is running inside reinforced bunkers.

DANIEL'S PROMPT

Daniel

We’ve previously discussed the intelligence community's use of cloud computing, security, and "stand-alone internets" for sensitive information. Given examples like AWS creating a cloud for the CIA and Microsoft’s collaboration with the Israeli government, how does it work in practice when major commercial cloud providers roll out products for governments and the intelligence community? How is that extreme level of data security, federacy, and physical infrastructure separation preserved to meet the most demanding requirements in the world?

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. I am Corn, and I am joined as always by my brother.

Herman

Herman Poppleberry, at your service. And man, do we have a deep dive for you today. Our housemate Daniel was actually listening back to some of our older episodes, specifically episode two hundred seven where we talked about open source intelligence, and he sent us a voice note with a really pointed question. He was asking about the intersection of the massive commercial cloud providers and the intelligence community.

Corn

Right, and it is such a fascinating topic because it feels like a total contradiction. On one hand, you have companies like Amazon, Microsoft, and Google that are the backbone of the public internet. They are designed for scale, accessibility, and sharing. And then on the other hand, you have the intelligence community, where secrecy, isolation, and physical security are the absolute top priorities. Daniel was asking how these two worlds actually mesh in practice. How do you take a platform built for the public and make it secure enough for top secret government data?

Herman

It is the ultimate engineering challenge, Corn. And it is not just a hypothetical one anymore. We are talking about multi billion dollar contracts that have fundamentally reshaped how spy agencies operate. If you look back to about two thousand thirteen, that was really the watershed moment. That was when the Central Intelligence Agency signed a six hundred million dollar deal with Amazon Web Services to build them a private cloud. At the time, it was revolutionary. People were asking, wait, you are going to put the nation's secrets on the same platform that hosts Netflix? I remember IBM actually protested that contract, arguing that a public cloud provider couldn't possibly meet the security requirements. But the C I A stuck with Amazon, and it changed everything.

Corn

Exactly. And I think that is the first big misconception to clear up. When we talk about the intelligence community using A W S or Azure, they are not just logging into the same website we use. It is not like there is a secret folder in the standard A W S management console labeled top secret. Herman, you have been digging into the architecture of this. What does the physical reality of a government cloud actually look like in early twenty twenty six?

Herman

It is all about the concept of air gapping and physical separation. In a standard commercial cloud, you have what we call multi tenancy. Your data might be sitting on the same physical hard drive or being processed by the same C P U as a dozen other companies. They are separated by software, by what we call logical isolation. But for the intelligence community, logical isolation is not enough. They require physical isolation. For the top secret regions, we are talking about data centers that are physically disconnected from the public internet. There is no wire, no fiber optic cable, no wireless signal that connects these servers to the outside world. They are often built in undisclosed locations, sometimes inside reinforced bunkers or what the military calls Sensitive Compartmented Information Facilities, or S C I Fs.

Corn

I have always loved the idea of an S C I F. It sounds like something out of a Bond movie. But these are real facilities, right? Shielded against electromagnetic interference, with their own power grids and water supplies.

Herman

Absolutely. They are designed to prevent what is called TEMPEST leakage, where someone could theoretically intercept the electromagnetic radiation from a computer monitor or a keyboard and reconstruct what is being typed. These facilities have incredibly strict biometric access controls. We are talking about iris scans, palm vein mapping, and multi factor authentication that would make your head spin. And it is not just one big room. Within these data centers, you have different zones for different classification levels. The Secret region is physically separate from the Top Secret region.

Corn

That is incredible. So, when an intelligence analyst logs into their cloud, they are on a completely parallel version of the internet. We have discussed these standalone internets before, like S I P R Net or J W I C S, but this is like taking the entire suite of modern cloud tools, the machine learning models, the massive databases, and dropping them into that isolated environment.

Herman

That is precisely it. And that is the value proposition for the government. Before this, the intelligence community had to build everything from scratch. If they wanted a database, they had to build it. If they wanted a search engine, they had to build it. But commercial tech moves so much faster than government procurement. By partnering with Amazon or Microsoft, they get to use the exact same tools that the world's best developers are using, but within their own private, high security bubble. And as of January twenty twenty six, cloud providers are making advanced artificial intelligence capabilities available in government cloud environments. The most advanced A I in the world is running inside air gapped bunkers.

Corn

But here is what I don't get. If these systems are truly air gapped, how do the cloud providers actually maintain them? How do you push a software update or a security patch to a server that has no physical connection to your main network? You can't just hit update and wait for the progress bar.

Herman

That is where it gets really interesting and, frankly, quite tedious for the engineers involved. They use what are called cross domain solutions. Imagine a digital airlock. When a software update needs to move from the low side, which is the unclassified commercial side, to the high side, which is the secret side, it has to go through a rigorous inspection process. Sometimes this involves a physical transfer of media, like a secure drive being hand carried into a facility by a cleared courier. Other times, they use hardware called data diodes. A data diode is a physical device that only allows data to travel in one direction. It uses light or a one way electrical path so it is physically impossible for data to flow back out. It is like a one way valve for information.

Corn

So the update goes in, but the secrets can't come out. But even then, how do you know the update itself isn't a Trojan horse?

Herman

You don't, at least not without checking. The code is scanned, re scanned, and checked for any vulnerabilities or hidden backdoors before it is allowed to run on the high side. They use automated tools, but also human reviewers. It is a massive logistical hurdle. But for the intelligence community, the trade off is worth it because they get access to massive computing power that they just couldn't replicate on their own. Cloud providers are making significant investments to expand their government cloud capacity and capabilities. That is enough to power substantial operations, just for government A I.

Corn

I want to touch on the point Daniel made about Microsoft and the Israeli government. This isn't just a United States phenomenon. We are seeing this globally. Here in Israel, we have Project Nimbus, which is a one point two billion dollar project to move government services to the cloud, specifically using Google and Amazon. It has been quite controversial, hasn't it? Especially with recent developments.

Herman

Oh, absolutely. Project Nimbus is a great example of the complexities of sovereign clouds. There have been concerns raised about the human rights implications of the contract, and there have been massive protests from employees at both Google and Amazon. It highlights the tension between a global tech company's values and the requirements of a sovereign state. When a government moves its data to a commercial provider, there are huge questions about data sovereignty. Even if the data center is located physically within Israel, what happens if the company is headquartered in the United States? Which laws apply? What happens if there is a political disagreement and the provider decides to cut off access?

Corn

Right, and that leads to the concept of the sovereign cloud, which seems to be the big trend for twenty twenty six. Governments are now demanding that these companies provide not just security, but total autonomy. They want the cloud to be operated by local citizens who have undergone local security clearances. They want the encryption keys to be held exclusively by the government, so even the cloud provider cannot see the data. We are seeing this with the A W S European Sovereign Cloud that just launched in Germany. It is physically isolated from the global A W S network and operated entirely by E U residents.

Herman

And the cloud providers are bending over backward to meet these requirements because the contracts are so lucrative. Microsoft has their Cloud for Sovereignty, and they use local partners like Bleu in France to ensure the infrastructure is operated by local entities. Oracle is doing the same with their E U Sovereign regions in Frankfurt and Madrid. It is a total reversal of the old power dynamic. In the past, the government held all the most advanced technology. Think about the early days of the internet or G P S. It started in the military and then trickled down to the public. But now, it is the opposite. The most advanced artificial intelligence and data processing tools are being developed by private companies, and the government is the one trying to catch up.

Corn

You are spot on, Herman. It creates this weird situation where the intelligence community is essentially renting their infrastructure from a private company. Now, to be clear, they aren't renting space on a public server. They are paying the company to build and maintain a private version of that infrastructure. But the intellectual property, the software that runs the cloud, still belongs to Amazon or Microsoft. So, what happens if there is a major security flaw found in the underlying code of A W S? If it is discovered on the commercial side, does that mean the secret side is also vulnerable?

Herman

That is the nightmare scenario. And it is why the security audits for these government clouds are so intense. Most people don't realize that when a company like Microsoft provides a top secret cloud, they aren't just providing the hardware. They are providing a massive team of cleared personnel who do nothing but monitor that specific environment. But you are right, if there is a zero day vulnerability in the core hypervisor code, the software that allows multiple virtual machines to run on one physical server, that could theoretically be exploited on both sides. This is why the concept of Confidential Computing is so important now. It uses specialized hardware like Intel S G X or A M D S E V to create a secure enclave in the processor. Even if the operating system is compromised, the data inside that enclave remains encrypted while it is being processed.

Corn

I remember we touched on this a bit in episode three hundred sixty one when we were talking about unified A I workspaces. The more we centralize our data into these massive cloud platforms, the bigger the target becomes. For a foreign intelligence service, breaking into a commercial cloud provider is like finding the keys to the kingdom. Herman, how are they handling the multi cloud aspect? I know the Pentagon moved away from that winner take all J E D I contract.

Herman

Right, the J E D I contract was cancelled and replaced by J W C C, the Joint Warfighting Cloud Capability. That one is a nine billion dollar deal split between A W S, Google, Microsoft, and Oracle. And just this month, the Pentagon announced they are gearing up for J W C C Next, which is expected to be even bigger and focus on third party marketplaces. They want to be able to move their workloads between different clouds to ensure they always have the best price and the latest features. It is about resilience. If one provider has a massive outage or a systemic security breach, you aren't completely dead in the water.

Corn

It is not just about storage, though. It is about the analytics. Imagine you are an intelligence agency and you have petabytes of satellite imagery, intercepted communications, and human intelligence reports. If that data is sitting in a bunch of disconnected legacy servers, it is almost useless. But if you put it all into a unified cloud environment, you can run massive machine learning models across all of it simultaneously. You can find patterns and connections that a human analyst would never see. That is the real power. It is the ability to turn a mountain of noise into actionable intelligence in near real time. And that requires the kind of scale that only companies like Google or Amazon can provide. I mean, think about the sheer number of G P Us needed to train a modern large language model. No single government agency is going to have a data center that can compete with what the big three cloud providers are building.

Herman

And that brings us back to Daniel's question about how this works in practice. One of the most critical components is identity and access management. In a normal company, you might use two factor authentication. In the intelligence community, it is way beyond that. They use something called attribute based access control. It isn't just about who you are, it is about where you are, what device you are using, what time it is, and what specific project you are cleared for at that exact moment. The cloud allows them to enforce these rules with incredible precision. So, if I am an analyst and I am cleared for project X, the cloud will only show me the data for project X. Even if project Y is sitting on the same server, it is cryptographically invisible to me.

Corn

But I want to go back to the physical infrastructure for a second. We mentioned air gapping, but what about the supply chain? If I am the C I A, how do I know that the servers Amazon is putting in my secret data center don't have a hardware backdoor installed during manufacturing? We have seen allegations of tiny chips being added to motherboards in the factory before.

Herman

That is a massive concern, and it is why the supply chain security for these contracts is so rigorous. We are talking about what they call a trusted supply chain. Every single component, from the motherboard to the smallest chip, is tracked from the moment it is manufactured. They often use specialized facilities where the hardware is assembled by cleared personnel. In some cases, the government might even specify that certain chips have to be manufactured in specific, trusted foundries. If you can't trust the silicon, you can't trust the system. And that is why the intelligence community is so involved in the design phase of these cloud products. They aren't just buying off the shelf. They are collaborating on the specifications.

Corn

So, let's talk about the actual migration. If you are a government agency with decades of legacy data on old mainframes, how do you actually move that into a modern cloud? It sounds like a nightmare. You can't just upload a hundred petabytes over a standard fiber line.

Herman

It is a nightmare. It is often called the lift and shift problem. But for the intelligence community, they try to avoid just lifting and shifting. They want to refactor their applications to be cloud native. This means breaking big, clunky programs into microservices that can scale up and down as needed. And to get that data into the cloud, they use some pretty extreme methods. Have you ever heard of the A W S Snowmobile?

Corn

Is that the literal truck?

Herman

Yes! It is a forty five foot long ruggedized shipping container pulled by a semi truck. It can store up to one hundred petabytes of data. They literally drive the truck to the agency's data center, plug in a massive fiber optic cable, load up the data, and then drive it to the cloud data center. For the intelligence community, they have specialized versions of these devices that are even more secure, with armed guards and G P S tracking. It is peak My Weird Prompts. The most advanced cloud technology in the world still sometimes relies on a literal truck full of hard drives. It is like that old saying, never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway. A truck can move a hundred petabytes in a few days, whereas even the fastest fiber optics could take months.

Corn

So, we have talked about the physical security, the air gapping, the supply chain, and the migration. But what about the people? You mentioned cleared personnel. How does a company like Microsoft manage thousands of employees who have top secret clearances? That must be a human resources nightmare.

Herman

It is a huge hurdle. These companies have had to build entire divisions that operate like mini intelligence agencies. They have their own internal security offices, their own polygraph examiners, and their own secure facilities for their employees to work in. It has actually led to a bit of a brain drain from the government. If you are a talented engineer with a high level clearance, you can make a lot more money working for a cloud provider than you can working for the government. It creates this revolving door between the intelligence community and big tech. And it means that the culture of these companies is slowly changing. They are becoming much more aligned with national security interests than they were twenty years ago.

Corn

It is a delicate balance. They want the innovation of the private sector, but they need the loyalty and secrecy of the public sector. I am curious, Herman, where do you see this going in the next five to ten years? Are we going to see a world where there is no such thing as a government data center, and everything is just a private region of a commercial cloud?

Herman

I think we are headed that way for almost everything except the most sensitive, core tactical systems. The efficiency gains are just too high to ignore. But I think we will also see a move toward the tactical edge. We are already seeing Google Distributed Cloud air gapped appliances being used by the U. S. Air Force and N A T O. These are ruggedized, transportable appliances that allow you to run cloud workloads in the field, even when you are completely disconnected. It is like taking a piece of the cloud and putting it in a backpack or a Humvee.

Corn

That is the real frontier. Bringing that massive computing power to the person in the field, in real time. It is such a fascinating look at the hidden architecture of our world. Most of us just think of the cloud as this ethereal thing where our photos and emails live. But there is this whole other version of it, buried in bunkers and guarded by men with guns, that is processing the world's most sensitive secrets.

Herman

It is the ultimate manifestation of the phrase, knowledge is power. And in the twenty first century, power is measured in flops and terabytes. I think we have given Daniel a lot to chew on. It is a complex topic, but the key takeaway is that the extreme security of these systems isn't just about better passwords. It is about a fundamental reimagining of how hardware and software interact, and a massive investment in physical isolation.

Corn

Before we wrap up, I want to pivot to some practical takeaways. Even though most of our listeners aren't running a top secret intelligence agency, there are some lessons we can take from how the pros do it.

Herman

Definitely. The first one is the concept of defense in depth. Never rely on just one security measure. The intelligence community uses physical security, network security, and data encryption all at once. For a regular person, that might mean using a password manager, plus two factor authentication, plus encrypting your sensitive files locally. And the second one is the idea of least privilege. Only give people, or apps, access to the specific data they need to do their job. Most of us are way too permissive with the permissions we give to our smartphone apps or our cloud services. It is worth taking a look at your privacy settings and tightening things up.

Corn

And finally, remember that physical security still matters. You can have the best encryption in the world, but if someone can walk away with your laptop or your backup drive, you are in trouble. Treat your physical devices with the same care you treat your digital accounts. Great advice, Herman. This has been such an interesting dive. I feel like I understand the cloud a lot better now, and also feel a little bit more paranoid, which is probably a good thing in this day and age.

Herman

A little healthy paranoia never hurt anyone, Corn! Keep asking those weird questions.

Corn

True that. Well, thanks to Daniel for the prompt. If you are enjoying My Weird Prompts, we would really appreciate it if you could leave us a review on your favorite podcast app. It really does help other curious minds find the show. You can find all our past episodes, including the ones we mentioned today, on Spotify and at our website, myweirdprompts.com. We have an R S S feed there and a contact form if you want to send us your own weird prompts.

Herman

We have some really cool topics lined up for the coming weeks, so stay tuned. We will be diving into everything from the history of synthetic biology to the weird world of deep sea acoustics.

Corn

I can't wait for that one. The ocean is full of even weirder stuff than the cloud. Alright, I think that is a wrap for today. Until next time, keep asking those weird questions.

Herman

See you next week!

Corn

Bye everyone.

Herman

Take care.

Corn

And remember, if you see a forty five foot truck parked outside a government building, maybe don't ask what's inside.

Herman

Unless you have a top secret clearance, of course.

Corn

Of course. Bye!

Herman

Take care.