Miguel Orellana
5/3/2025

Cracks in the System: Why We Should Be Worried About Cyber Threats to Critical Infrastructure

(1) Introduction: We're Building on Shaky Ground

I've been thinking about how everything we rely on like power, water, and transportation is hooked up to digital systems now. It makes life easier, sure, but it also opens up a ton of ways things could go wrong. These systems weren't built for the internet age, but now they're connected, and that's a problem.

Looking at this through a philosophical idea we discussed in class the Short Arm of Predictive Knowledge it's clear that we don't really know what's going to happen in the long run. We keep building more complex systems and just assume we'll be able to handle it later. But that's risky, especially when we're talking about stuff like hospitals and power plants. If those go down, the effects can be massive.

(2) One Weak Link Can Bring the Whole Thing Down

Critical infrastructure is super important it literally keeps society running. But it's also fragile now because everything is connected. Remember the Colonial Pipeline attack in 2021? A ransomware gang got in through the business side of the network, and the whole pipeline got shut down. That caused gas shortages across the East Coast. All that chaos, just from one cyberattack.

The scary part is how easily something like that could happen again. These systems were never designed to deal with hackers or ransomware. We're just trying to bolt security onto outdated tech, and that's not enough.

Plus, these systems all rely on each other. If one fails, it could mess with everything else. And we're using more AI and automation now, which adds another layer of unpredictability. If something goes wrong, or the AI gets tricked, we might not even understand what's happening until it's too late.

(3) We Think We're in Control But We're Not Really

A big issue is that a lot of cybersecurity planning is focused on what's already happened, not what's coming. We patch holes and fix problems once they show up, but that kind of thinking doesn't help us stay ahead.

Take those old SCADA systems still being used in places like water treatment or energy. They were built ages ago without cybersecurity in mind, but they're still running today. Instead of rebuilding from scratch, we just keep adding more software and tools on top. Honestly, it's kind of like trying to fix a leaky roof with plastic wrap.

Now we're throwing AI into the mix, thinking it'll solve everything. But sometimes even the people building those systems don't fully understand how they work. What if attackers learn how to trick them? What if they mess up without anyone noticing? That kind of stuff is really hard to predict.

Miguel Orellana
5/3/2025

(4) Nobody’s Totally in Charge

Another problem is that it’s not always clear who’s supposed to be responsible for keeping critical infrastructure safe. In the U.S., for example, a lot of these systems are run by private companies, but if something goes wrong, it becomes a national security issue.

So who’s in charge? The government? The company? Both? Right now, it’s kind of messy. Sometimes companies don’t want to invest in cybersecurity unless there’s been a major incident. And by the time the government catches up with new rules or regulations, the threat has already changed.

Technology moves fast, but laws don’t. That gap creates opportunities for attackers to take advantage before we even know what’s happening.

(5) Conclusion: We Can’t Predict Everything—But We Can Be Smarter

The big takeaway from all this, at least for me, is that we’re not as prepared as we think we are. The Short Arm of Predictive Knowledge reminds us that we don’t have the ability to fully understand or predict where all this is going. But that doesn’t mean we’re helpless.

Instead of pretending like we can anticipate every threat, we should focus on building systems that are resilient, so even if something goes wrong, the whole system doesn’t collapse. That means adding backup systems, keeping some parts manual, and making sure people not just machines can step in when things go wrong.

We also need better cooperation between companies and the government. They have to work together and share info instead of waiting for a disaster to act.

I get that it’s hard. You can’t just replace every system overnight, and nobody wants to spend money on something that might not happen. But we need to at least admit that what we’re doing now isn’t enough. If we keep going like this, we might create problems we can’t fix later on.

We don’t need to predict every single thing. But we do need to think a lot harder about how we’re building the future and who’s going to deal with it when it breaks.

Miguel Orellana
5/3/2025

Reference

The attack on Colonial Pipeline: What we've learned & what we've done over the past two years: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, August 23). https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years