**THE BROOKINGS INSTITUTION**
**The *TechTank* Podcast**

**"Navigating private-sector cyber operations under Trump administration policy"**




**Monday, November 23, 2026**

*Guest:*

LEONARD BAILEY
Former head of Cybersecurity Unit/Special Counsel for National Security,
U.S. Department of Justice,
Computer Crime & Intellectual Property Section

*Host:*

STEPHANIE PELL
Fellow,
Center for Technology Innovation,
Governance Studies,
The Brookings Institution

[music]

[00:00:00] **CO-HOST NICOL TURNER LEE:** You're listening to TechTank, a biweekly podcast from the Brookings Institution exploring the most consequential technology issues of our time. From racial bias in algorithms to the future of work, TechTank takes big ideas and makes them accessible.

[00:00:22] **GUEST HOST STEPHANIE PELL:** Welcome to the Tech Tank Podcast. I'm guest host Stephanie Pell, a fellow in governance studies at the Brookings Institution. The Trump administration's national cyber strategy promised to unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our capabilities.

Exactly what the Trump administration had in mind with respect to such private sector cyber operations was, however, unclear. Then, in August, the administration issued a national security presidential memorandum titled Expanding Capabilities to Combat Transnational Cyber-Enabled Crime. In this memorandum, the administration lays out a framework for enlisting qualified private sector companies to conduct cyber effects operations and cyber surveillance operations under contract with the Department of Justice and the Department of Homeland Security.

But even as this memorandum provides more detail regarding how the administration envisions the private sector's participation in cyber operations, some fundamental questions persist. Why hasn't the private sector seized on various efforts to give US companies more authority and opportunity to conduct offensive cyber o-operations against cyber threat actors?

And are we likely to see greater involvement by multinational communications providers in such operations under the framework provided by this presidential memorandum? To help answer these questions, I'm joined by Leonard Bailey, who spent 33 years at the Department of Justice, where he managed cyber policy as an associate deputy attorney general, senior counselor to the assistant attorney general of the National Security Division and head of the Cybersecurity Unit, and special counsel for national security in the Criminal Division's Computer Crime and Intellectual Properties Section.

He recently published a paper that gets at the heart of these questions titled "The Clear, the Muddy, and the Insoluble of the Administration's Cyber Operations National Security Presidential Memorandum." Welcome, Leonard. Thank you for joining me.

[00:03:07] **GUEST LEONARD BAILEY:** Thank you. So pleased to be here, Stephanie.

[00:03:10] **GUEST HOST STEPHANIE PELL:** So to start off, can you give us some history and background on the debate surrounding private sector engagement in offensive cyber operations?

You know, what have been the issues at play? And can you define and distinguish offensive cyber operations from the ways in which the private sector has traditionally assisted the federal government?

[00:03:37] **GUEST LEONARD BAILEY:** Of course, Stephanie. So this is an evergreen topic that dates back at least a dozen years and, and certainly longer.

If you don't mind, I'd like to start with just a quick level-setting explanation of the law in this area. So the principal federal hacking statute, the Computer Fraud and Abuse Act, Act 18 USC 1030, um, in general prohibits three things. It does more than this, but in essence, this is what it does.

One, it prohibits intentionally accessing the computer without or in excess of authorization. Two, it prohibits intentionally accessing a computer and causing damage without authorization. And three, it prohibits knowingly transmitting a program, information, code, or command and intentionally causing damage as a result without authorization.

So each of these activities are things that we would anticipate would happen during a, a cyber operation potentially. Um, the most important thing, though, for the CFA in this discussion is that there is no self-help, um, or self-defense provision for the private sector. There is an exception for the government that permits the government to engage in lawfully authorized intelligence, law enforcement, and protective activities that would otherwise violate the statute, but, but not the private sector Now, when I was at DOJ, I recall being on numerous, numerous panels where we had vigorous debates over whether to amend the CFAA to allow private sector, um, hack back, that is allowing the private sector to respond to intrusions or attacks by accessing or attacking the perpetrator, or, um, having DOJ perhaps interpret the CFAA somehow to, uh, incorporate common law defenses like, like necessity.

And those, those efforts never really gained much purchase. There was a serious attempt to amend the law between 2017 and 2019 that, um, Representative Graves drove, which was the, the Act of Cyber Defense Certainty Act that had some bipartisan, um, support, but never got to the floor. And, um, I guess just this year, July and August of this year, you had a couple of bills, um, that were, uh, proposed that were rooted in, um, Article 1, Section 8 of the Constitution authorizing Congress to grant letters of marque and reprisal that would allow private sector parties to seize subjects and, um, foreign goods.

But as I understand it, those are not advancing, um, at this point at least. Uh, so that's sort of the, the legal construct. Um, to further answer your question though, I'd like to just also make it clear that This isn't new, that the government has been partnering with the private sector on cyber operations, uh, for at least 15 years.

I remember back in April of 2011, I was at the Computer Crime and Intellectual Property Section when the Coreflood operation was, was executed, um, and in that the DOJ successfully disabled a botnet in a malware family that was being used as DDOS tools first and then became a keystroke logger for, for banking credentials.

But in doing so, that was the first kind of disruptive operation the government engaged in. And if you looked at the press release for that, you would see that thanks were given to Microsoft and the Internet Systems Consortium for their help there. Uh, and if you go back over the years, you'll find dozens of takedowns, acknowledged cyber operations conducted with the private sector's help, Gameover ZeuS, Qilios, Avalanche, Emotet, um, over three dozen operations since 2020.

And in many of those, if you look at the press release, you will also see, um, thanks to the private sector. The last thing, in answer to your question, is, uh, historically, while the private sector has helped and supported these operations with malware analysis, information sharing, um, even lent infrastructure, they haven't been the one conducting the operations usually.

And that's where the NSPM is different. It's asking the private sector to actually be what I would call trigger pullers, um, the ones who are actually executing the operation.

[00:07:44] **GUEST HOST STEPHANIE PELL:** So let's talk then about the efficacy of cyber operation, specifically in terms of strategic versus tactical effects and the kinds of companies that are in the position to help the government achieve strategic effects against malicious cyber actors.

[00:08:07] **GUEST LEONARD BAILEY:** Great question. So I think one lesson the US government has learned over time is that cyber operations have many different applications. Um, now we understand from the military that, you know, there are many contexts in which, uh, cyber operations can be used to support and enable kinetic operations. Um, just see the government confirmation, uh, from Cybercom that they had participated in the January 2026 operation in, in Venezuela to capture Nicolás Maduro.

Um, but there are also intelligence applications. In some instances, they may support diplomatic efforts. And most relevant to this conversation, given the scope of the NSPM, they can be used by law enforcement for a variety of purpose, from evidence gathering to disruptive operations, um, to disable criminal infrastructure Now, sticking with the criminal context, so DOJ and US law enforcement have generally enjoyed very good tactical success in using cyber op- operations against transnational criminal organizations, um, things like ransomware groups or, or dark markets or botnets.

The challenge is that those are really kind of bespoke operations that are built to address the specific tactics, techniques, and procedures, TTPs, of a particular group. Now, these can be very effective against a targeted group, but they come with some limitations. Often, the bad guy can actually pivot quicker than the government can respond to kind of operational changes.

And that's, that's not meant to be a criticism of these. I think those are important tools, but, um, I think two things to remember are that, one, it's in the nature of crime fighting that you don't eradicate crime, you manage it, right? Ideally, um, in ways that result in meaningful reductions, but you don't, you don't eliminate crime.

That's not really the way that works. Also, uh, there are things that go into a well-executed cyber operations, um, that ensure that they are technologically sound, that there are no unintended consequences, that there's adequate legal review and deconfliction, and those things take time, um, and those aren't things that attackers or intruders need to do or need to worry about.

So there's always a little bit of a disadvantage that the government has in these, um, in these efforts. Now, to use cyber as a strategic tool, and when I say strategic, I mean one that can, let's say, influence an adversary's decisions and actions as well as drive your planning and decision-making I guess I'd say you need a few things.

You need to be able to generate effects that are sufficiently predictable, controllable, and, and credible to be integrated into a plan that achieves your ends. And the problem is that cyber often, well, one, your capabilities are perishable. You'll, you may burn that, that resource, um, you know, once you've used it.

They're hard to scope. That is, the effects could be delayed, they could cascade unpredictably, or they may fail silently without you knowing it, and they can be hard to signal because you can't really demonstrate a capability without actually using it. Um, and so even with the smartest minds and best tools, which the US government by and large, you know, does have, there are strategic limitations to cyber operations, at least at, at this point.

Um, so somewhere along the path to becoming a strategic tool, we, we probably have to look at how we routinize collaboration with the private sector, um, and make them something that we can do in a more turnkey fashion and at scale.

[00:11:42] **GUEST HOST STEPHANIE PELL:** So on that point of turnkey operations that can scale, to date, we haven't seen the large multinational telecommunications, cloud, and internet communications providers jump on the bandwagon to obtain more legal authority to engage in offensive cyber operations.

Do you have a theory for why that is? Can you talk about that?

[00:12:08] **GUEST LEONARD BAILEY:** Sure. Uh, and I'm glad you, you called out specifically, like, the telecommunications and cloud and kind of communications providers, because I think that's exactly where we would really need to start. Um, you know, rather than at the endpoints, these providers who operate in the middle, who are able to do things on their own networks at scale in a turnkey way using authorities that they have and they're familiar with using.

However, you know, as you pointed out, uh, and as I note in the, in the piece, these aren't the companies that are leading the charge on, on, on this. And so why is that? So when I, when I was head of the cybersecurity unit in the Computer Crime and Intellectual Property Section, um, at Justice, and maybe even more since leaving Justice, I've had the opportunity to speak to CEOs, CISOs, CIOs, folks generally in the C-suite, uh, C-suite about cybersecurity, cyber defense.

Um, and one thing that's been impressed on me is that managing risk is one of the prime tasks that any business, large or small, has. It's how a business makes money. Uh, a business, you know, generally wants risks to be deliberate, understood, proportionate to the expected returns or benefits. Um, now there are many things that might whet a private sector company's appetite for taking risk, a potential windfall, perhaps, you know, large profits, opportunities for growth.

Um, but I can tell you one thing that generally doesn't encourage risk-taking, and that is uncertainty. Um, and the adoption of cyber operations right now, particularly for large and

multinational companies where, you know, their line of business isn't cybersecurity or cyber defense, really jumping into cyber operations is full of uncertainty.

And in general, I'd say the government hasn't done a great job of eliminating that, that uncertainty while trying to encourage companies to, to engage in it.

[00:14:06] **GUEST HOST STEPHANIE PELL:** So let's fast-forward then to recent policy issued by the Trump administration under the National Security Presidential Memorandum, or NSPM. Can you tell us about this new framework, um, and what it attempts to do?

[00:14:26] **GUEST LEONARD BAILEY:** Of course. Uh, so as you said, um, August 12th of this year, the Trump administration issued a new National Security Presidential Memorandum, or NSPM, that's focused on expanding the government's use of the private sector's cyber capabilities to augment the government's ability to interdict what the NSPM calls, quote, "cyber-enabled transnational criminal organizations."

Now, the focus of the NSPM, um, is on cyber-enabled transnational criminal organizations. Um, and in discussing that, it expressly carves out, does not apply to entities that are not, quote, "an institutional part of a foreign government or wholly operated under a foreign government's direction." Um, so it immediately carves out actors like those the government thinks are responsible for Salt and Volt Typhoon and other incidents that are attributed to nation state actors.

So what does that leave? Well, the, the foundation of the NSPM is built on EO 14390, um, which was signed in March of 2026, called Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens. So that suggests that the primary cyber threat the N-NSPM is, uh, was drafted to address is fraud.

Like, you know, for example, the scam centers in Southeast Asia that have become of, of great concern. But that doesn't mean that it couldn't be applied elsewhere, right? So, um, it could also include ransomware groups, for example, the, at least those that are not run by foreign governments, and we'll have to see how, you know, as this is implemented, they deal with criminal groups that are arguably proxies for nation-states.

But something else the NSPM must do to operate is it repurposes something called the National Coordination Center, um, which was created by a EO last year, uh, 2025, that was focused on immigration, and places the NSPM's operations under the control of two executive directors who are at the NCC, one from DHS and one from DOJ The NSPM requires companies who want to participate in the NSPM to do several things.

One, they have to sign a contract with DOJ and DHS to conduct any operation under the NSPM. Two, under those contracts, they have to operate under, quote, "Control and oversight of the United States government." Um, they will receive information from federal, state, local, tribal, territorial agencies that is intended to enable them to propose cyber operations to the

NCC, and then they must put up a one-million-dollar bond, which kind of serves as a gating function for the type of groups that can, uh, join.

But it also interestingly replicates what was required for privateers receiving letters of marque and reprisal back in, in the 1800s. The government also has some obligations under the NSPM. First, the NCC is supposed to establish minimum standards for participating companies, um, that would touch on things like technical proficiency, um, performance of cyber operations, uh, their security at facilities, um, personnel vetting, competence, reliability.

The executive directors must also approve in writing the private entities' operational plans and then also conduct operational deconfliction with the interagency, including, you know, military and IC agencies. There's a reporting requirement that the NCC has to create for [00:18:00] participating companies for information about the activities and impact of foreign transnational criminal organizations.

And finally, DOJ has the responsibility of ensuring that operations directed at US persons or that otherwise implicate US government obligations under the Constitution, federal laws, or international law, uh, receive the necessary authorization, now whether it's a warrant or order or something else. The last kind of cap here, I think, that makes, uh, that warrants mention is that, um, there's a limitation on the type of operations that can be executed under the NSPM.

Um, they cannot generate, quote, "critical outcomes," which the NSPM defines to mean something that results in the loss of life or serious injury or that rises to the level of use of force or armed attack under international law. And that still leaves you a lot of room to maneuver, and it's a pretty high threshold.

[00:18:50] **GUEST HOST STEPHANIE PELL:** So now I really want to delve into the arguments you make in your paper, and specifically reference part of its title, "The Clear, The Muddy, and The Insoluble," to discuss whether the framework you've described addresses four buckets of risk relating to private sector engagement in offensive cyber operations.

So if you would, uh, perhaps start with giving us a high-level overview of these buckets of risk that you identify.

[00:19:20] **GUEST LEONARD BAILEY:** Sure. Um, so I mentioned that there are these categories of risk that all businesses weigh in decision-making, and I guess I'm positing that there are some that are particularly important and salient to cyber operations.

What I've observed is there are sort of four categories of, of kind of risk that are, are weighed that affect the willingness of a company to collaborate with the government. The first is just government support. Is the government agreeing that the, that the company should do this, or are they gonna come after them with civil, criminal, or regulatory sanctions?

Two, uh, If the private sector were to act, you know, working with the government in this case, what authorities would it be using? Uh, and here I, I have proposed kind of there's a spectrum

of partnership that could exist from the, the low end being each independently acting in their own, you know, on their own accord, using their respective authorities in their own interests, um, climbing next to information sharing activities, which is just providing information in support of cyber operations.

This is, you know, happens all the time right now, generally mostly from the private sector to the government, but there's that next level. Above that is, uh, coordination, where either or both may notify the other of, of its actions. Um, they aren't depending on the other to do anything, but it provides sort of plans so that the other can take action perhaps.

Now, this is different than information sharing that, like, you're informing someone else so, so that they can leverage that information to do something even though you aren't, you know, telling them what to do or cooperating with them. Above that, you have collaboration, which is kind of synchronizing what you're doing, working in concert with the other so that your actions are actually designed essentially to benefit each other, to support each other, um, but you're still using your own authorities.

And finally, there's direction, where the government, and usually it's the government directing the private party, to take some action, and this would be action the private party would not otherwise conduct, and they would be acting really under the government's authority as directed. Now, there's a legal significance to where you fall on that spectrum.

Um, the closer it is to government direction, the more likely a private party may be considered an agent of the government or a state actor, and that has some legal consequences. The NSPM puts private parties at that end of the spectrum, uh, of directing, um, its actions specifically. So, I'm sorry, that's a lot in risk two.

So risk three is, uh, just, um, there are questions that have dogged cyber operations for some time, which is what is the legal liability that's faced by a private party who engages in cyber operations? What statutory or common law protections may they assert to protect them from, from legal consequences?

Um, and the fourth risk is the kind of operational commercial risk that a company shoulders when it conducts cyber operations, maybe fallout from customers, perhaps harm to its brand, perhaps prosecution by foreign authorities. So those are the risks that I'm focused on.

[00:22:23] **GUEST HOST STEPHANIE PELL:** So can you talk about now, and you, you go on with some deep analysis, um, of this in your paper, but interested in hearing about the extent to which the administration's framework offered in the NSPM addresses these four buckets of risk.

What is clear, what is muddy, and what is insoluble?

[00:22:47] **GUEST LEONARD BAILEY:** Yeah, so with a tip of the hat to Clint Eastwood and the good, bad, and the ugly, um, kind of bin these in these clear, uh, muddy and insoluble

categories. So what's clear is government support here, um, right? So there's no question that the government here is saying, "We want the private sector to expand its role in cyber operations," and that's evidenced in the NSPM itself.

Um, and that's clear at least under this administration, right? So it's an NSPM, it's not a law, and another administration may have a different view of that. But for now, that checks the box of, of government support, addressing that uncertainty. They also have concreteness on what authorities will be used, right?

We know that the NSPM says, "You will do this using government authorities. We will be directing you." And so that's, that's also crystal clear. The third category is where we start getting into the muddy, um, and that's with the question of legal protections. So the NSPM doesn't directly speak at all to legal protections, um, but I think you can infer that it's designed to extend certain legal protections to private parties by requiring them to operate as government contractors, and in doing so, that they would be able to take advantage of criminal and civil legal protections that are extended perhaps to an agent of the government under the CFAA, and civil protections under doctrine established by the Supreme Court in two cases.

I can mention in a moment, Boyle versus United Technologies and Yearling versus W.A. Ross Construction. Um, so starting with the CFAA, the, the idea is that by acting at the direction of, of law enforcement or intelligence, uh, a private party can step into the shoes of the government under 1030F, which I mentioned, you know, at the outset of, of the show.

But here's where the muddiness comes in. The statute refers to law enforcement intelligence agencies only. It doesn't mention an agent of the government or someone acting on behalf of the government. Now, that omission isn't dispositive. Um, I mean, that doesn't mean that this cannot apply in those situations, but there are other statutes that are arguably analogous that do expressly speak of agents of the government.

Um, the DMCA, Digital Millennium Copyright Act, for example, has a provision that, that looks like this, and there's, you know, a canon of statutory interpretation, um, that kind of touches on this. It was kind of tried out in 1983 in, in Russello versus United States, but it suggests that where Congress includes particular language in one section of a statute but omits it in another, it's presumed that Congress acts intentionally and purposely in either including or excluding that, that language.

Now, this is not a perfect case of that. This is not the same statute. These are arguably in somewhat analogous similar statutes, but it does raise the possibility that a court could at least raise an eyebrow at the lack of, uh, express mention of, of an agent. Um, now even if that failed under the, um, CFAA, there are some common law fallbacks that one could argue.

There's a public authority exception, um, where a government official, um, may direct a private party to act, and in doing so extends some type of, uh, you know, common law argument that they're permitted to do that, that act. Um, and there's also something called entrapment by estoppel that, that might, might operate here.

Um, although, you know, there have been some cases, or at least one case, that raises the question of what exactly lawfully authorized means under 1030and whether that presumes the existence of a warrant rather than merely acting at the direction of a, of a, of a private, private party. Now, living in the real world, uh, let's say that these defenses fail.

One could ask realistically, what are the odds of the government actually prosecuting a company that is working with the government at its direction? And the, the truth is, you know, it's probably remote. It'd be kind of Orwellian for the government to prosecute a company in that state. But that doesn't mean that there couldn't be potentially civil liability, um, if a party were harmed in that.

Now, kind of pivoting to, to civil liability, there are some contractor defenses that the Supreme Court has found, um, Boyle versus United Technologies and Yearling versus W.H. Ross Construction. These are similar, but they are slightly different. Boyle, uh, actually has a three-part test for its application.

One, you have to have reasonably specific instructions from the government. Two, a contractor has to have followed those instructions. And three, the contractor has to warn the government of any dangers that it knew about that the government did not. The thing about this particular type of, of protection is that It seems to require strict compliance with a contract, like the description of a contract.

And you could debate how well that's gonna work with cyber operations, which often kind of fluid. Um, they can change on a dime. They may require some creativity as they're unfolding. And the more latitude, uh, exercised by an operator, the more likely they may fall out of having followed instructions under Boyle.

Similarly, you could say, well, maybe the government should just draft, you know, very general instructions, but then you have prong one, which says there have to be reasonably specific instructions. This makes the use of Yearling a similar but slightly different, um, protection, maybe more, more attractive.

Uh, under Yearling, a contractor does... if it does what the government lawfully authorized it to do, um, and then acts within the scope of the government's authorization, it receives, you know, legal protection. So it's less focused on adhering to the specific instructions that are, that are given and more to whether it's operating within the government's authority.

One catch is it, it, it leads to the question of what is the government's authority and, you know, a question about what, what's government's authority to delegate this operation to a private party, which might be part of the inquiry. Um, the second thing is that it confers, according to the Supreme Court earlier this year, they clarified that this does not confer derivative sovereign immunity.

It is a merits defense, which means that rather than sort of absolute immunity, you may still have to go through discovery, motions, and even a trial before you can exercise the, the protection, which means there are some, some downsides to all that.

[00:29:34] **GUEST HOST STEPHANIE PELL:** I mean, that's, that's going through a litigation.

[00:29:38] **GUEST LEONARD BAILEY:** Essentially, right, and all the cost and resources that, that would, that would attach.

[00:29:42] **GUEST HOST STEPHANIE PELL:** And then you've got, um, the insoluble.

[00:29:46] **GUEST LEONARD BAILEY:** Yes. Then you've got, and then you've got the insoluble. So this is the category of things that, uh, basically There are issues that could not be clarified by Congress or no government official could, could resolve.

There's just no solution under US law. And some ex- simple examples of this are things like risk of retaliation by a transnational criminal organization, or maybe more seriously, the concern that you are risking some legal action from activities you're c- engaged in in a foreign country under the domestic criminal or, or civil laws of, of that country.

And we know from the UN Trade and Development, uh, database that 90% of the 195 countries in the world have some form of, of cybercrime law, meaning probably a law that touches on unauthorized access to a computer. And that means for an SVM that contemplates foreign operations that will occur under f- you know, in foreign countries and therefore maybe may trigger foreign laws, that companies may be subject to those laws.

And there's little that the US government can do to prevent a foreign country from charging a participating company or its employees with a crime under their own laws. We may refuse to extradite someone, for example, but, um, that would still have a impact on their vacation plans.

[00:31:14] **GUEST HOST STEPHANIE PELL:** And I think you also talk in your paper, there are some real reputational and broader business risks involved for transnational companies who may seek to engage in cyber operations on behalf of the US government.

[00:31:32] **GUEST LEONARD BAILEY:** Completely right, yes. I mean, I think one lesson from the USA Patriot Act, uh, and how that was received in Europe is that you may find that consumers in a foreign market, and foreign governments as well, may not love the idea that companies are operating within their space who not only may be engaged in cy- uh, cyber effects operations, but may be also engaged in cyber surveillance operations on behalf of the US government.

So yes, there's also that other layer of risk.

[00:32:06] **GUEST HOST STEPHANIE PELL:** So given the risks and uncertainty that you've described, what kinds of companies do you think will take advantage of this framework?

[00:32:22] **GUEST LEONARD BAILEY:** That's really the whole game, isn't it? Uh, I mean, I think time will tell. My guess is that you will have smaller boutique firms that specialize specifically in cyber operations and developing cyber tools that are staffed by former NSA or intel operators who have a higher tolerance for risk and maybe not as well lawyered as larger multinational companies that may be, you know, champing at the bit to do this.

I suspect, though, that, like, your larger multinational companies that are subject to the laws of other countries will think very hard before signing up. And it's not just, as you mentioned, it's not just the potential of, of criminal civil liability, it is the commercial impact that, that I think might just as much give them pause before jumping in.

[00:33:13] **GUEST HOST STEPHANIE PELL:** There was one line of your paper that, that stuck with me, and that was, the more lawyers that a company has, the probably the less likely they are to avail themselves of the new possibilities presented by this framework.

[00:33:29] **GUEST LEONARD BAILEY:** It's always the lawyers. It's always the lawyers. Um, but, but I do think that actually a long time the lawyers will be, will be the business concerns.

[00:33:38] **GUEST HOST STEPHANIE PELL:** Fair enough. And so taking all of that into consideration and, and the, the types of companies that you think are more likely to take advantage of this framework, do you think that this framework, this broader policy that, that the Trump administration is trying to enable will actually expand capabilities that can be brought to bear against malicious cyber actors?

[00:34:08] **GUEST LEONARD BAILEY:** So let me say at the outset that, uh, one, I want to applaud the administration for taking the swing because, you know, this is a topic that's been around for a long time. We spent a lot, lot of time wringing our hands about what may be possible here, and this is really the first serious attempt to propose a model.

Um, that said, I think the NSPM as it's drafted already illustrates some of the difficulties of creating a program of this sort, uh, some of the things I've gone through and we've discussed already, and I suspect that further challenges will kind of arise in the implementation phase as it's unrolled, as it's rolled out.

Let me also say, though, that I think this is a capacity that we need to have. I think that any serious policy for security of US critical infrastructure and assets needs to include the capacity for combating and interdicting cyber threats, and that, that needs to be built out. Even so, I tend to think that shoring up our defenses still carries a better return on investment than attempting to go out and knock down threats.

So, I mean, at the end of the day, I think that, that this, assuming that com- some companies take, take the government's invitation here, that we'll have things that prove tactically useful

However, I think anyone who believes that this is gonna move the needle and result in a meaningful reduction in the cyber threat landscape that we face is going to be disappointed.

[00:35:40] **GUEST HOST STEPHANIE PELL:** So you've referenced, uh, of course, the need to shore up our networks. Um, I presume critical infrastructure is included in that. Along those lines, what are, in your views, given the decades of experience you've had at DOJ, specifically looking at cyber policy, what kind of engagement on the defensive side is, is fruitful for the government to have with the private sector?

[00:36:12] **GUEST LEONARD BAILEY:** Yes. So I'll loop back to something we, we touched on a, a few minutes ago, and that is I do really think that the electronic communication service providers and the cloud providers are really at the center of, of, or, or should be at the center of this, this discussion. Again, they're the ones who can do these things at scale with their own existing authorities on their own networks, and they're kind of a logical linchpin to conducting these types of operations in a routine manner, again, at scale.

I also think that the model for this, I would choose a different model. I would choose a model that, uh, had the government provide and identify priorities, not direct the private sector to do what it, what the government wants it to do, but tries to align interests and gives the private sector more leeway to respond using their own authorities in their own interests.

I think the private sector does very well at protecting their own assets. Those interests are often aligned with the US government's. Having a means of, of identifying priorities, but allowing each to operate in a, you know, a coordinated but, but still separate manner, I think would be maybe less fraught.

It would be maybe not as well orchestrated as being able to direct a party. I think, though, it would avoid some of the problems we've talked about and maybe result in something that was more palatable to the private sector.

[00:37:45] **GUEST HOST STEPHANIE PELL:** So any other thoughts or issues we've not covered that you'd like to mention today?

[00:37:49] **GUEST LEONARD BAILEY:** So I guess, I guess the closing thought is, um, I think we need to be sure that we are being thoughtful about how we're implementing cyber policy and where we're investing what is a limited amount of resources and attention that we have to a complicated problem. I think some of the drive for having offensive cyber capabilities, not all, but some of it, comes from an understandable desire for what I would call revenge or street justice.

There's this, this great bit of dialogue in a Brian De Palma film, I'm gonna date myself, The Untouchables, uh, where you had the FBI going after Al Capone. You had Sean Connery playing a grizzled Irish street cop who explains the Chicago way. It's, "He pulls a knife, you pull a gun. He sends one of yours to the hospital, you send one of his to the morgue.

That's the Chicago way." And that's, that's great dialogue, but I'm not sure it's great cyber policy, uh, particularly for a country like ours that has such asymmetric vulnerabilities compared to the rest of the world in digital. And even, even with the best offensive cyber capabilities on the planet, which I think we have, we also have the most digitally dependent society on the planet, and we have a lot to lose from a world in which sort of disruptive attacks become the norm.

Um, so I'd say we better be careful about what vision of cyber defense we're espousing and how well-suited it is to US interests.

[00:39:24] **GUEST HOST STEPHANIE PELL:** Well, on that note, we'll leave it there for today. Leonard, thank you so much for joining me. You can learn more about this topic by reading Leonard's paper, "The Clear, the Muddy, and the Insoluble of the Administration's Cyber Operations National Security Presidential Memorandum."

And you can explore more in-depth content on tech policy issues at TechTank, accessible at brookings.edu. This concludes another episode of the TechTank Podcast. Thank you for listening.

[00:40:01] **CO-HOST NICOL TURNER LEE:** Thank you for listening to TechTank, a series of roundtable discussions and interviews with technology experts and policymakers. For more conversations like this, subscribe to the podcast and sign up to receive the TechTank newsletter for more research and analysis from the Center for Technology Innovation at Brookings.