AI Cybersecurity After the Executive Order: What's Next?

Fri, Jun 12, 2026 12PM

SUMMARY KEYWORDS

AI cybersecurity, executive order, vulnerability scanning, patch distribution, threat actors, zero-day vulnerabilities, AI tools, cyber defense, technical debt, public-private partnerships, ISACs, national privacy law, quantum computing, fraud and scams, cybersecurity challenges.

SPEAKERS

Kate **Charlet**, Senior Director for Privacy, Safety, and Security Policy, Google
Elizabeth **Chernow**, Associate Vice President, Public Policy, Comcast Corporation
Shane **Tews**, Nonresident Senior Fellow, American Enterprise Institute (moderator)
Prem M. **Trivedi**, Director, New America's Open Technology Institute
Ari **Schwartz**, Managing Director of Cybersecurity Services and Policy, Venable LLP

Shane Tews 00:09
So the good news is I'm very excited about this event. If we've done this even 10 days ago, we would be talking about completely different topics, because so much has happened in the last 10 days. Part of that is artificial intelligence, and part of that is how are we managing cybersecurity into this process, and the thing that I want to note is, when we're talking about these things, is remember when we're talking about cybersecurity, we're just not talking about the act of cybersecurity, we're talking about all of these systems, all these IT systems that isn't necessarily tech, but everybody who uses technology, and I'm going to highly encourage you to ask questions. So, I mean, I've been doing cyber for a long time, and there days I look at these things, and I'm like, I don't even know exactly what this is. To be very honest, I used Claude this morning. I put a bunch of notes on things I was working on, and I was

like, you know, I'm not so sure about some of these acronyms. Make me an acronym referral chart, so just in my notes I had 47 acronyms. That's how it goes. So, anybody wants my acronym chart, either come see me or I'll send it to you, because that might be helpful. Because they love to make up acronyms fast and furious, and if you were dealing with ag stuff on one day and then cyber on the next day, you may have that one acronym in your head, and it's not the same thing, so we are.. we've got a great panel today. So I'm joined by Liz Chernow from Comcast and Prem.. sorry, I can say your last name, okay? Because I feel that conversation.. New America Open Technology Institute, and Ari Schwartz from Venable, and Kate Charlet from Google, who just came in this morning, so she's off of red eye, so she's probably going to be really smart, be gentle when it comes to the questions. So the couple things that we are going to focus on is the presidential executive order that came out on June 2, and then how it kind of dovetails into the things that have happened previously, not only just in cyber, but with this administration, there was the it comes from AI foundational things that are that are not completely clear where we're going to land on this, so we're going to have a good discussion about that. I'm also going to offer, even though this is a panel discussion, if we're talking about something and it really grabs you, feel free to raise your hand, so you don't have to wait to the end for questions, just in case you feel like you really want to engage on that point, so there we go. Okay, so we are going to start with a will with just kind of the threat landscape on how is the AI fund, how is AI fundamentally changing the cybersecurity threat environment right now, and and what are we doing about some of these things, especially since Mythos came out, because I feel like Mythos was such a big game changer, and I know other companies will say, like, we were already worried about these things, but maybe Anthropic just made us say it out loud, and then they just, they're too little out on the market. There's a little bit of a thought about that, but just the AI fundamental question, I'm going to start, actually, Kate, with you, because I know you deal with this very much on a day-to-day basis,

Kate Charlet 03:02
yeah. Thanks, and thanks everybody for joining. I'm Kate Charlet. So, I lead Google's public policy teams for privacy, safety, and security. Previously at the Department of Defense Cyber Policy, and one of Google's units is a Google Threat Intelligence Group, so I think starting on the threat question is a good one for us, and I think we have been - it's clear we've been very much talking, we've all been talking now about AI and cyber security, and this conversation has really ramped up, and that is a very good thing, but it's worth remembering that this is a trend line, a threat trend line that has been taking place for several, several years. So our threat intelligence group has been monitoring this threat. I think early on you were seeing threat actors adopt AI, kind of in the context that we were all initially adopting AI, in terms of making our workflows more efficient, maybe making phishing emails a little bit higher quality, more have more grammar, fewer red flags, but what we've been seeing over the course of time is that AI-driven cyber threats are becoming more and more sophisticated, and they threat actors are using AI across the threat lifecycle, whether that's finding and exploiting vulnerabilities, whether that is helping to create exploits. So, in our most recent report, last month we published that the first we saw the first time that an actor had found and exploited a zero day vulnerability using AI, so we're starting to see that we're starting to see threat actors use. AI to do agentic orchestration, so scale and speed, kind of, you know, perhaps in real time evade defenses or use autonomous malware, so have payloads that work autonomously that interact with the victim device or execute on commands without necessarily going back to to a human, so we're seeing the capability increase, and I would maybe say not to just like we should get into the defense side of this, because I think the news is not all bad in that AI tools, if

we do it the right way, and we spend the time driving and investing in AI tools for cyber defenders, really poses the opportunity to flip the advantage towards the defenders, but that's going to take work, and I think there's going to be, in the short term, quite a bumpy ride over the next 12 to eight months, you know. While, while that shift takes place,

Shane Tews 06:08
Ari, you're the next.

Ari Schwartz 06:10
Yeah, so Ari Schwartz, I event about also the executive director of the Cyber Security Coalition. I've spoken to three of our members that were part of Glass Wing, the mythos first run, think probably most of our members are have been involved in some way, but three of them were able to give me some details, so I just give you a sense of what's different today. So this is, let's last six months, right, we're not talking about like changes beyond that. So one company told me, and all of them were in this range, but one gave me some very specific numbers of that two years ago they found 50, there were 50 known exploits for new vulnerabilities for their, for their software, for all their software, so they had 50 big patches to basically to put together very, very quickly under Mythos is finding them, it's now 40 a day, right? So that's 300 times change the change there in terms of what they have to do, and they had less staff to do it right already, so than they did two years ago, so that particular company, so that just gives you a sense. The other thing is, in terms of days to exploit, so we used to think of, like, well, some of these will take two weeks to exploit. This one is like a bigger one, maybe it'll take some months to exploit. When Mythos brings you vulnerability, it brings the exploit code with it. It is so, if it has, when we say so, it is exploitable at the time that they find the vulnerability. So that means that it's not theoretical. No, none of this is theoretical the way that when we talk, we, when we used to talk about vulnerabilities, some of it was, some of it was theoretical. Now it is all instantaneously something that they must fix immediately, so just to give two examples of what makes things different.

Shane Tews 08:06
Great, and Liz, maybe you can talk a bit to the where that comes in at the level of being, you know, Comcast and an operator, because it's you have so many people, your customers are riding on this, and you've got a level of protection on a Comcast customer here in DC, and you know, I just know that Comcast says that somebody's trying to break in my system. I say, cool, they know what's going on, and I don't question it. Sometimes I do look it up, only because I'm a DNS geek, and I like to look at the URLs. But yeah,

Liz Chernow 08:32
for sure. Thank you, Shane. I'm Liz Chernow, I'm Associate Vice President for Public Policy at Comcast here in our DC office. And a little bit about us. We operate the largest converged network in the nation. Half of all US broadband traffic crosses our network. So, we support over 30 million customers with over a billion devices, that includes residential, small, and medium businesses, and government, state, state, and federal local government customers, so we are one of the biggest critical infrastructure operators in the US, and we, you know, we know that we have a lot of assets that we need to protect, and we take that responsibility very, very seriously. We go to great lengths to secure our networks and the services that we provide to our customers by deploying best in class cybersecurity defenses and

practices throughout our network, and we focus really on three north stars when it comes to our security products and practices. We operate on zero trust principles across our entire enterprise. We use, and we use AI to improve our security as well, so we're also building security into all of our products. Within this context, AI presents both challenges and opportunities for us. On one hand, you know, we leverage AI to detect and manage the complex threats that, you know, are trying to get into our network. We make tools available to our small and medium business customers to empower them to secure their networks as well, and to help them with that. On the other hand, we receive a lot of cyber attacks, both AI-generated and otherwise, and with these new frontier models, you know, Mythos really was the first that we were seeing, but you know, we fully expect more to be coming at us. It made it clear that we need to ask ourselves, you know, what. Who needs to be able to have these capabilities before the capabilities are in the hands of attackers, because if an attacker can use a frontier AI model, and as Ari said, you know, with the exploitation code readily available, then as a defender, we need to be able to find issues early and harden our networks against these issues.

Shane Tews 10:52
Could all the panelists bring your microphones closer to you, please? Thank you. Great. Okay.

Prem Trivedi 11:00
Yeah, so Prem Trivedi with the Open Technology Institute at New America think tank here in DC, and we were.. you guys hear him? Is he okay? Yeah, okay. Work on a number of tech policy issues, primarily at the intersection of AI governance, privacy, and data security, and responsible data use. And so, if you're operating at that intersection, you can't ignore everything that's happening in the sort of scary and to some extent promising environment in cybersecurity that AI models, advanced frontier models, are driving right now. I think you know, Shane, you wrote a piece in late April talking about what Mythos teaches us about the bill that's coming due on decades worth of accumulated cybersecurity technical debt, which I think is worth highlighting. Right, so we've got, we've got these known sets of vulnerabilities where often newer, modern tools are stacked on top of older systems. There are lots of legacy vulnerabilities, and think about power grid, think about maybe hopefully better dealt with in banking, but they're, you know, go down the sectors where you think about that's critical infrastructure that has both national security implications as we think of them from a state perspective, but also national security and people security implications as we think of them from an ordinary consumer and American perspective, and what mythos has done, right on the scary side of the house, is I think make those decades of accumulated technical debt now a live attack surface, and so it's sort of enabling at industrial scale the exploitation of those decades of accreted and slowly patched, if patched at all, vulnerabilities. Right, we have some - we have these sort of crazy numbers. Ari spoke to them a little bit right, so mythos and glass wing partners using mythos surfaced something like 10,000 plus critical flaws in a period of weeks, I think, and the sense that, like, what is being discovered as a vulnerability is, to Ari's point, immediately weaponizable really constricts rapidly, I think, the question of how much time you have to respond to those vulnerabilities, and so I think I share the optimism, right, that I think advanced AI cyber tools pose offensive challenges. They also pose defensive potential, but I think what's interesting from the perspective I sit in is we also know that the patching problem is an institutional coordination problem, it's a human resource and system problem, and that's where I think my highest level of fear is, not that we aren't going to have some nerd, harder technical tools to employ

on the defensive side, but that we're really going to have to work hard to address coordination problems that have bedeviled our systems for decades, that's what scares me most.

Shane Tews 13:36
So, I'm just going to add, so technical debt, I did write a blog about this a couple weeks ago, and the challenge is, especially the older you are as an institution, the more possibility of having technical debt, because you have a lot of legacy systems that at some point might have made sense, but they're still hanging around, and then they may be lesser used, so somebody's not doing the patching on them, or they didn't get updated. Sometimes the companies go out of business, and you still have them in your system, and those are the ones that the criminal and criminals love those because it's like I forgot I had a window on the third floor and there's you know it's really accessible for my neighbor's house and you didn't close it so that that's become a huge challenge so and I'm going to move to Kate because you're like this is where we get to the defensive posture if you're on the defensive posture, you're having to look at everything to swat at all the time. If you're the criminal intent, you just need that one access point that gives you the space. So, talk about how much more challenging that has come in the last couple months.

Kate Charlet 14:33
Yeah, and I'll talk also about the potential to flip that right. So, I think on the defense side, AI for cyber defenders, which is, I think, where we should all be really thinking about how to accelerate that. There's a short term and there's a long term in this. In the short term, you know, using AI tools for vulnerability detection, that's what we've all been talking about. That's what Glasswing has been for. Sure, and then to your point, you then remediate it, you patch it, but you still run into the problems of classic patching. You have to create the patch and apply the patch, but AI tools can also help to automate that as well to generate and apply the fixes. That's something we are working on. We have a tool called Code Mender, so it's not just identifying the vulnerabilities, it's actually fixing them. So, I think that kind of research and that area is a really important potential, but then over the long term, you see, well, you could embed AI in the code, the software code development process, like embed it in the Azure building code from out of the gate, making sure that it's more secure out of the gate, so you see over that long term the potential for the vulnerabilities to just not come into being in the first place. Obviously, that's a, that's the, that's the goal. That's easier said than done. But then you can also see, just as we're seeing threat actors use AI to move laterally to automate aspects of the threat attack cycle. You can also use AI for defenders to automate and understand environmental risk quickly, move to mitigate that risk to see threats as, as, as they arise, and so you can, you see these opportunities to have more of an environmental protection using AI for cyber defense,

Shane Tews 16:50
and so, Liz, when I think about you all, you have to look at this from both sides, because you're not only delivering content to people and the ability to use the interwebs, internet, you also have them going the other direction, and they may be creating one of your smaller clients, actually may be causing part of the challenge, so you have a very large task at hand there. How, and you do it very well, but I know that it's just like gotten that 10x probably isn't even enough, you know, maybe 100x harder. So, how are you guys managing through that,

Liz Chernow 17:22
you know, we, we have a very deep bench of cybersecurity professionals, and we

Shane Tews 17:27
Can you speak up just a little bit? Thanks. Yeah, better.

Liz Chernow 17:31
And we, we do use AI tools to, to harden our network and to secure our customers, you know, we agree that that patching does remain an area that that could use some support, and I think you know there's there's the vendor side, and there's also the open source side. It's a complicated problem, and it's really good to see that we're having a lot of those conversations now to come together now that we know how much more patching is going to be needed.

Shane Tews 18:00
Are you shaking your head on the open source?

Ari Schwartz 18:03
Yeah, I mean, I agree with several things that she just said. The main writing patch, getting AI to write patches, is, you know, it's the opposite side of this equation, right? And you could do that also, you know, rewriting. In the past, we used to say, like, oh, well, if we could get rid of our code, is written in an old language that has a lot of known problems with it, we can't rewrite our entire code base to move it up. Well, now you can rewrite your entire code base. It is a project that AI can help you do. So, there are some things that are structurally long term very, very positive things for the defenders can do. There's some problems involved in that, which is, I mean, you have to take resources off of other things to make some of those longer term things happen, and to address those issues. And it's more, it seems to be, I mean, we're finally having this discussion here about how expensive it actually is to use the AI, and that means not just expensive in terms of, like, you know, getting people to use the right prompts and things like that. The actual tokens to use it is expensive, and the defensive side of this, the writing code, etc. seems to be more expensive than the finding of the vulnerabilities, does so from what people have been telling me, so there's concern on that side, and then there's also the role that a person has to be with the AI is harder on that side as well, so it's more expensive from a resource side on both ends of this, and a lot of EOS, a lot of executives that have been thinking about AI, it's hard for them to get their head around. Well, we also need more people with using more AI, which is going to be more expensive than we thought it was. All at the same time, like it's not that hasn't really sunk into a lot of the calculation here of, and certainly hasn't sunk into Wall Street, where they're saying, "Oh, you should cut jobs so you can save money and invest. And AI, instead, like that's just not the way this is going to work, if we're going to get to the point of actually being more secure. Do

Shane Tews 20:07
you have anything to add on the defensive side?

Prem Trivedi 20:10
Yeah, just a couple points, kind of echoing and synthesizing what folks have said. I mean, I think so. What's the potential on the defensive side? So AI allows lots of institutions, companies to do continuous

discovery, continuous triage, and then to generate patches as well, right? Not just flag of vulnerability across all the surfaces in an organization. That's something that even the best teams working with the best tools, say 12 to 18 months ago, couldn't match, right? At that at that kind of scale, and presumably that accuracy. I think it's really interesting just to sort of quickly pick up on Ari's point, we are seeing right, we keep having these sort of business and market conversations about an AI bubble, which I'm not here to speculate on, but the point being companies are pouring tremendous amounts of money into developing these models, right, and so they're getting more and more advanced, money keeps pouring in. I had this question in my mind, and I had a bit of an instinct, which you seem to be confirming, which is that the defensive side of the house now is going to become incredibly expensive, and that is just going to be a resource challenge to layer along, you know, sort of human coordination challenges we've been talking about. Be interesting to watch. I think there's a lot of defensive potential that this panel has emphasized. Cost is an interesting thing to watch.

Ari Schwartz 21:16
One of our members called it, called this summer patch summer, instead of patch data, we're going to be getting patches all the time, but it also means rewriting a lot of code and pulling people off that we're doing new features to products and taking them off of that to redo the code and rewrite things and to work, use AI in a positive way and get them trained in the right way to use AI in that way, so that that is like where a lot of people are headed right now. Just

Prem Trivedi 21:38
a quick, you know, that's a really good point. Quick two finger on that too. Is like we are in a very commercially competitive AI frontier model, and even sub frontier model race, and so those are going to be some tough questions for companies to make, right? Which is like, how much time do we take off of next gen product and AI integration, next model development, and how much we put into, you know, sort of that defensive side of the house is going to be interesting, and I think you're going to have downstream users of frontier models that are going to face their own set of how much time do I spend innovating with these tools and bringing go-to-market products out. How much time do I spend dealing with accumulated technical debt?

Liz Chernow 22:14
And just one point on the patching, too. I spend a lot of time talking to our cybersecurity teams, and it's not just like, you know, putting a band aid on a cut, you actually have to, you know, validate the patch, make sure it works, make sure that when you're patching in one place, you're not taking down something else. So it is a very resource-intensive process.

Shane Tews 22:33
There's two analogies I really like, because I think it helps visualize for those who are visual thinkers. One is that it's like shining a black light, like all of a sudden you think you've got everything clean, and then you shine a black light, and you're like, oh, I've missed a lot of things here. And then the other one is like, as far as it's also like you just dropped the keys to every system in the room and said you might not, you know, just go ahead, the keys there, go ahead. I mean, it's like staying at a hotel and every door just opened and you're like, okay, well, that is that. How are we going to expedience is very important, so part of this is a timing issue. So I'm going to get to the government parts of this, because

this is where it gets very interesting, especially for you all in the room. So the recent president's executive order creates a clearing house, which Ari's very excited about. He can talk about the clearinghouse for a long time, but it coordinates the vulnerability scanning, validation, patch distribution we were just talking about, and it's very important, but if this isn't, again, just an IT, this isn't just a tech company problem, it is critical infrastructure operators throughout, so hospitals, banking has issues on this, now we're talking about a lot of coordinated effort that we need to do in this space, and as probably you all know, in the room, we've had some challenges with CISA with funding and the things that we are asking them to do. So, Ari, since you're a big fan, can you just give us the baseline on why the clearing house is important and how it functions?

Ari Schwartz 23:52
Yeah, so I mean, it's actually a lot of the critical infrastructure companies are most excited about it, even more than the tech companies, but some tech companies are excited about it too. The so let's, let's go back to your analogy of like dropping the keys everywhere, right? So I'll put it, put that in a, in a little more of a context, context, context, which is so critical infrastructure company says, you know, to to a cyber security company that is the member of Glasswing, you know, we have, how many new patches are in your patch download, and they say 50, and he's like, how can it be 50? Like, you usually have two or three. Well, this is the first of the, and it's going to be 50 for a while. I said, well, we can only deal with three, right? We only, because we have to test all of our systems all over the place, and make sure that this works with that, so like, and I can't have, and the response back from the company is, it's not going to be just us. Every piece of software you're running is going to have 50 new patches tied to it every week for the foreseeable future, so you have to change the way you're doing patching and have a conversation. Information about that with other people that are dealing with the same thing, so that maybe you can find out where there are areas where things have gone down, or where things have, where things have not interacted well, or where patches, which patches we really need to prioritize, because on top of this, the scoring system for vulnerabilities has been known to be not great for many years, and

Shane Tews 25:24
what is the scoring system for those who aren't familiar? Just, just give us a two sentences. Yeah,

Ari Schwartz 25:30
so that CVSS is the, is the current scoring system that's used, and there's several, several groups of people that are involved in coming up with the scores. This is involved in DHS, and this is involved in some way as well to bring things into the National Vulnerability Database, and all this is sort of run by MITER as a contractor, right, and they have a board that kind of oversees some of this as well, and so they take in the vulnerabilities and they rate them based on how much impact they think that this thing's going to have and how likely it is to be exploitable, right. Well, we've already said the vote, if a vulnerability comes with for Mythos, it is exploitable, right. And then there's also a whole bunch of the problem with mythos that we've seen, is from what, from what I've heard, about 15% of the vulnerabilities that they have are these chained vulnerabilities, which basically take low, what we used to be considered low-scoring vulnerabilities, and chain them together, so that they become critical, like to the highest level of things that need to be addressed. So you have to figure out a way to break the chain of these low, low vulnerabilities, et cetera. So there's sort of a complex feeling series here, where

you're like, well, this we scored this low, but it's not about that, it's about the risk behind it, right, and so you saw, and the DHS just put out a new Binding Operational Directive to agencies, so this gets to get a little bit ahead here, basically talking about the risk and the risk involved, and part of that is because they're saying don't just look at the score, the CVSS score, you have to put it in context in a broader context, and so a clearing house could certainly help people to put things into a better context in terms of that risk, as well as share just the sharing of the patches and things like that,

Shane Tews 27:21
it's always already brought us to one of the reasons why I needed an acronym chart was I wasn't sure what the BOD was, and the first thing I read, I was like, what's the BOD, Binding Operational Directive, so there's a

Ari Schwartz 27:32
reason that they, we came up with that term, Binding Operational, original P, they want to use guidance, but guidance is used like by 12 different places, so they try to come up, I'm sure you all been

Shane Tews 27:40
in many rooms where you had to decide that one word, and then you fight about it for an hour, that's what we ended up, but the other part of the BOD is the it requires a three day remediation vulnerability, which there have been there been decades of conversation about the timing and why that's a challenge. I actually met with a woman, I think she was from Estonia a couple years ago, and she said, "I don't understand why it takes you guys so long. We can do it in four hours, and I was like, "You can kind of walk across your country in four hours, so I can see why maybe you can hand deliver it. So it's, it's a real.. there's a lot of challenges, and we'll get into that, but just sort of.. so we put that in context, because I realize this is some for some of you, this is a lot of new information coming over. So, any other thoughts on where we're headed on the clearing house, and

Prem Trivedi 28:25
I think I can, I can take a stab just looking at the text of the EOS, trying to get reminded, right? What does it say about forming an AI cybersecurity clearing house, volunteer collaboration with the AI industry operators of critical infrastructure? All sounds good. What are they going to do? Coordinate and deconflict scanning for vulnerabilities, and then we move into discovers and validate such vulnerabilities. Right, validation is incredibly important. Coordinates and prioritizes remediation and distribution of vulnerability patches. So, as I read that clause, I really hope, right, that the second half of that sentence, or the middle, the middle third, and then the last third of that sentence gets a lot of institutional airtime and development in the clearing house, because to the points we've been hearing on the panel so far, I think probably whatever the coordination mechanism is, whether it's the sort of ISAC model we've seen, presumably faster and more flexible clearing house that's being stood up now, they're probably not going to lack for information routing to one another about vulnerabilities. What would be great to see as well is information routing about how have we used AI to automate, you know, the management problems on the patch side, the human institutional manage side. Like, let's have sharing on that, right? So, as much sharing, I think, on remediation as on spotting the vulnerabilities and sharing them is going to be important. That sounds obvious, but I think it's, it's the second problem

is the harder problem, and so my hope is that that's where the clearing house is going to put a lot of institutional oomph.

Shane Tews 29:48
Liz, and Liz, is this an opportunity? Do you want to talk about your paper to the Aspen Digital paper as well? No,

Liz Chernow 29:54
I would love to. Thanks, Shane. So, as I mentioned, one of the issues that we've been grabbing. Dealing with is just, you know, as a critical infrastructure provider, making sure that we have access to these technologies before they fall into the hands of adversaries, and sort of thinking through a way to do this, because you know, as we're seeing these frontier models, AI models are surfacing vulnerabilities at scale, so my colleagues and I, including our Chief Information Security Officer, New Brunswick Davis, we recently laid out in a paper for the Aspen Institute, Aspen Digital, a responsible advanced access model for critical infrastructure providers that takes the deliberations away from a single organization, so you know the way that it works right now is you have a company, I don't mean to pick on Anthropic, but Grass Lane, the Glass Wing program had gotten a lot of attention, obviously, but you have one individual company that no matter how well intentioned, there are 16 critical infrastructure sectors, and there are a lot of interdependencies between the critical infrastructure sectors that one organization sitting in its own corner of the economy is not going to fully understand and appreciate, and so what we're calling for is some sort of process that takes it out of the hands of an individual actor and makes it a transparent and public and accountable process in partnership with the sectors and partnership with the sector coordinating councils to determine which critical infrastructure actors are best positioned to be able to have early access to these models because what happens now is you have a national security issue, right, with these advanced frontier models. So we want to really make sure that the collective defense of critical infrastructure enables operators to respond to the vulnerabilities and coordinate ecosystem-wide efforts before the vulnerabilities can be exploited by those who want to cause harm.

Shane Tews 32:04
Kate, any comments on all this stuff? New stuff, I

Kate Charlet 32:07
mean, from our perspective, we welcome the executive order. It really does set out a goal to put AI in the hands of cyber defenders, and we're committed to doing our part to do that. We have our AI threat defense capabilities through Google Cloud, that puts what I was talking about, Code Mender, looking at the ability to not just identify but fix big sleep finds vulnerabilities whiz the same way you're talking about the, you know, looking across an environment where those vulnerabilities can add up, you know, our whiz capability helps to look at that and identify really what are those exposed attack paths and sever those attack paths, so I think the, you know, yeah, we welcome the executive order and look forward to continuing the conversation and the collaboration on

Shane Tews 33:08

it. To kind of put this in context, I'm actually going to tell you a story on AI. So, I came from a tech company that had an entire security division, and we took everybody in the company took security, very, very - it was critical, I mean, there was no question about it. It was top priority. So, when it came to risk, it was be thought of it as a number one risk. And then I joined the think tank, and one of my friends from the cybersecurity space called me and said, you know, it's not just you, they're doing it to all the think tanks on Massachusetts Avenue, because, you know, the Chinese think that we're all an arm of the government. Not true, but he said, so they're actually, they've broken into your system, and I can see that they're monitoring your systems at AEI right now. I'm like, cool. Okay, so I walk up, and I'm going to talk to the head of IT, but along the way I run into the former president of AEI, Arthur Brooks. You guys might know he did Oprah recently, and Arthur Brooks stops me. He goes, "What are you working on? And I said, "Well, the Chinese are in our system, and he goes, "Cool, they're reading our papers, full stop. Like, I couldn't get him to care after that, and I was like, Arthur, we had an IT problem, and he was like, it doesn't sound like it to me. So, you do, depending on where you are, there's a differencing of opinions as to how important this is, and sometimes it's monetary, some of it's just a very lazy, fair, hey, you know, that's not bothering me today. So, we had to go from that, so I'm going to go from that to the one of the challenges that we're seeing. We've got, we've got this clearing house, which is great. And then, for those who are familiar with the information sharing advisory committees or councils, the ISACs, which are housed over the Department of Homeland Security, there are layers to them. Very beginning of this process was in the telecom space back when they broke up AT&T, because think about it, old school AT&T, they could, they could just have a relationship with the government, they knew everything was going on, they was easy, and then they broke up AT&T, there were new companies, and they had to figure out, all right, how do we manage information flow, and then they created it, was it telecommunications, it was the first ISAC, and then during COVID, I mean. Several of them. Now we created an IT ISAC, and people started to realize it was separate from telecom. There became one, actually, for hospitality. So there's a hospitality ISAC, because they realized there were all these similar things they could learn. If you were a restaurant, you were a hotel, you were a shopping mall, where you had to start thinking about things. So it started to really raise the level of interest of people, information sharing, but there's two challenges to information sharing that lawyers think about. One is liability, and the other one is can they get indemnified from that liability. So, the ISACs have that capability. It's one of the reasons why you join one of these information sharing capability things, and so the president in the earlier, because the last was November, announced in one of the plans that he wanted to create an artificial intelligence AI ISAC, and now I feel like there's a delta between what we're seeing in the EO and the ISAC, and part of that is it goes around the incident reporting requirements, and depending on how important this is to you, back to my example, might be very important, and others will be like, I'm not going to take the risk, I'm not going to, it's just not that important to my industry, or maybe it hasn't been made out how important is to it. So, any thoughts on the kind of challenge of all these tools that are being brought forward, and which ones you feel like you should really be using, and which ones the government should be promoting?

Liz Chernow 36:19
So, one thing that I, that I would like to mention, just, you know, in this environment, we're seeing some really creative and collaborative models for public-private partnerships. The communication sector recently launched, it's called the c2 ISAC, which works as a complementary body to the communications sector ISAC, and the c2 ISAC is focused solely on cyber security threat information

sharing, whereas the original Com ISAC does both physical and cyber security. Our sister is actually the vice chair of the organization. I know Ari has his new, his members' new organization as well. So I think you know, coming up with these new forums and elaborating on the public private model that we're seeing, you know, just so we are able to do this in a way where there is liability protection and robust information sharing is really critical.

Kate Charlet 37:16
I'm interested in Ari's take on this question too, but I don't necessarily, I don't see the ISACs and the EO as in conflict or overlapping. I mean, there's a need for vulnerability handling where existing kind of disclosure processes aren't, you know, aren't suited for whatever reason, and there's a need for a broader set of information sharing. I do think that you know there are issues that an AI ISAC could discuss. Adversarial distillation of models is an example of that, but also aware that AI threats are not limited, you know, they're not happening in just an AI world like they're happening in the financial sector, in the health sector, and all the other critical infrastructure sectors, where there's a need for ISAC, so just making sure that information sharing is happening at kind of all the levels that it needs, needs to happen.

Ari Schwartz 38:16
I mean, I think they're both a little confusing, because they're both, both, they're actually the first, the AI, the first AI EO that the Trump administration put out had the AI ISAC in it, and this new security EO has this has this clearing house in it, so and both of them are written at a very high level, so I think people are seeing what they want to see out of both of them, and so if and there are visions, certainly that you could have where these two are totally clashing, and then there's visions where they are exactly the same thing, so it's hard to know, so I don't want to say state anything with like a so strong, because it depends on how these things are rolled out more than how what they, what then what each of our individual visions of them is, I would say the people that I talked to, there's there's there was concern originally about the idea of the AI ISAC, because it was the way that it's written in the EO, it is run by DHS, where the ISACs that have been successful have almost all been private sector created with public sector partnerships, right? Where, so, and so this idea of, well, oh, DHS is going to create this, is going to create a AI ISAC caused some consternation in that discussion. That's not to say that it has to be done that way, or that it has to. They can't just have it as a partnership. It has been made more complicated, I think, for them to do public-private partnerships, though, because Secretary Nome canceled the advisory body for critical infrastructure to work with CISA. What's called the CPAC, since she said they canceled it in like March, and then in April she said within the quarter - this is in 2025 - within the quarter will come back. It still has not come back, and she's no longer the secretary. So we are expecting it to happen over the summer that we will have something that we'll have that public private partnership. I think that will bring a lot more comfort to people about how this thing might work and how the coordination might work with it within the ISAC. If, and we'll be able to have a better understanding of what CISA's role really is in that ISAC, but meanwhile I think that the idea of pulling together this clearing house and figuring out what we want to do with the clearinghouse, and then we can figure out a role for the AI tech as it comes together, could make it more work very seamlessly, as Kate sort of described. So,

Prem Trivedi 40:49

yeah, so lots of interesting stuff to pick up on in the response, and I'll just, I'll take one thread from your question, which is, What are the incentives that you want to see to enable maximum sharing of information, right? Whether it's a clearing house, whether it's an ISAC, I think traditionally what we've seen is the importance of safe harbors and liability protections. Right, I don't align with industry on everything in the tech policy space, but I do align quite a lot with the need to say, look, if you're going to ask companies to potentially take on exposure to liability, to take on reputational risk in sharing information, I guess, to some extent, perhaps competitive sensitivity and proprietary information as well. Right, then you're going to need to also build some legal protective mechanisms into that architecture to ensure and incentivize people want to come forward to the table with their problems, right. And that's I'm trying to up level this a little bit for the audiences that are really in the weeds technically, and those that might not be. It makes intuitive sense, right? Why it is an uncomfortable thing to do as an institution or an individual to say, I've had this problem, I've either fixed it, I don't know how to fix it. This is the nature of the problem I'm sharing with you all, so that you can figure out how to deal with it as well, but also to help me deal with it. Like, if you put that in a very human individual context, it's a vulnerable thing to do. It is also, from a corporate structure perspective, a vulnerable thing to do. So, I think this question of how do we maximize the incentives to do this in an open way, and then to share information about what the problems are and how to remediate them, incredibly important. So, I also like Ari, don't pretend to know, I just, I can't figure it out, and there's not that much text to figure it out from what exact relationship is between the clearing house model and this EO and the ISAC model and the earlier EO, but I think the point that there should be genuine public-private partnership, and as a civil society rep, maybe we'll get to this a little bit later, some role in the overall kind of sharing and remediation and policy prioritization environment for civil society as well. I think those things are important. Wouldn't want it to see, and I just want to kind of just pick up

Ari Schwartz 42:43
on the point that you made about the safe harbor we have that in place, right? That's the Cybersecurity Information Sharing Act. And if there's one thing I would say to the staffers here, Congress, the one thing you could most important thing to do is to reauthorize the Cybersecurity Information Sharing Act. It applies to AI vulnerabilities as much as regular vulnerabilities. They're the same types of vulnerabilities. We know that it works. It's been, it's been in place now for 11 years. The reauthor, it had to be reauthorized last year, and Congress did it for months at a time, rather than just doing it for 10 years again, or just doing it forever. But that would be the one thing that Congress can do is to reauthorize the Cybersecurity Information Sharing Act for a long period of time.

Liz Chernow 43:29
Ditto.

Prem Trivedi 43:31
Plus one, plus one,

Shane Tews 43:33
for those of you that's the CISA versus CISA 15 that you might be following in your offices. Okay, great. So we have about 15 minutes left, and then two more questions for you, and then we're going to open it up to the room, so be thinking about what you want to talk about. So, you kind of led there, so you, if

you could tell this room the single most important thing you can do. So, we've got CISA, is there anything else that they should be doing? Is there new legislation? We have Chairman Older Multi put out a bill this week, we had senate had some serious hearing yesterday about this, actually, in the banking committee, so it's beyond just it thought, you know, it's all the other industry people as well. So give the people in the room some counsel here.

Ari Schwartz 44:11
I do, I mean, that bill, the amenity bill, the one thing that I will point out, I liked about it, it has a security section, I think it's good, and that section has an open source viewpoint, which you raised very briefly at the beginning of this, and open source is a real problem here, because they don't have the kind of funding or attention, so when you find a vulnerability there, it can take a very long, long time to get a patch, so having an exploit right immediately, and we know it's in open source, and it's affecting 80% of all code base, like that seems like something we want to prioritize to fix, and there's if there's no one there to do it, we're in a big trouble. So the idea of like, how do we get resources into open source, how do we get people that code people that do code to go and work with them, how do we get money for them to do to use AI tools like we were talking about before, I think that's all in. Going to be important in this discussion,

Liz Chernow 45:02
and I would add to that, you know, the older note to each try-hand bill contemplates an early access regime for certain open source maintainers. The executive order contemplates an early access regime for federal agencies. We think that, you know, this is a really good start and important steps in the right direction, but it's still critical that critical infrastructure organizations have early access to these technologies as well.

Kate Charlet 45:31
I would say maybe from a stepping back from a broader perspective, you don't have to be using the absolute like frontier to really make progress on AI for cyber defense, and so looking at ways, whether through procurement or supporting digital modernization efforts, efforts to use the cloud software as a service, platforms as a service, all those things are going to help put AI cyber tools in the hands of defenders, and I think that's a priority.

Prem Trivedi 46:10
That last point, good points here to pick up on. I mean, that last point from Kate is important too, because I think, and I don't have now the site handy, but it was either, I think, an anthropic or an Open AI report that basically said we found all these vulnerabilities, but like many of the ways to fixing some of them still are relatively basic, so there are a lot of areas where we need to throw nerd harder problems, more powerful tools from a cyber defense perspective. Cannot afford to forget the sort of rudiments of cybersecurity that we have seen in the last couple of decades be the sources of catastrophic hacks. I think that's a fair point, specifically to your point, like what should Congress do? I think, Ari, I agree with what you're saying, like fund and staff that remediation layer, particularly for open source vulnerabilities. I think building institutional capacity through resources, there is something Congress can certainly do. And then I'll offer a larger point that's agnostic about specific legislative vehicle for it, because I think it's also a political and a messaging point, and I said it a little bit at the

beginning. This is a really important time in the cybersecurity space, and dealing with the vulnerabilities and the challenges we've all been talking about to unite the consumer protection and the national security constituencies around consensus on the need to move quickly and to coordinate, right, because I think, depending on where you sit, depending on the institution that you staff or sort of care most about, you think of this as a potentially, you know, a hard security problem, the type that you, that calls to mind nation exploiting and sort of the geopolitical competition context, and you're absolutely right, it's that right, it is also very much vulnerability exploits are very much going to be consumer harm areas. It's going to be the people who are, you know, denied loans, the people who are defrauded. It's going to be power outages from cybersecurity vulnerabilities that affect people in businesses. And so these are, I think, like it makes sense at some level that in a specialized context you think national security and the associated architecture and equities here, and you think consumer protection and the associated equities and architecture here, but I think this is a moment where we've got to also build bridges across those constituencies and to tackle cyber security vulnerabilities at scale and the human coordination problems that go with them. So that's the broader point I wanted to make as well,

Shane Tews 48:19
and then in adjacent only in that from a legislative perspective, it's adjacent, but the question of data security or privacy, I think of it as data security, because I think privacy is an emotion. I also think that we should have a national privacy bill, and one of my other colleagues at AEI thinks, no, we've done a great job, finance has got their things, health is theirs, so we have varying points of view. Thoughts on is a national privacy bill something that would help this process as well, because you'd have more symmetry in the information focus. The whole point, there's two reasons to steal things online, or is basically, is you want the data, but you really want the data because you want the money, or if you can just straight up steal the money, it's easier, but a lot of times the data is the money, so thoughts on that.

Liz Chernow 49:03
Yes, we need a national privacy law, like the Secure Data Act.

Shane Tews 49:10
Anyone else want to weigh in? Just nod. Strongest one

Prem Trivedi 49:12
on the need for a comprehensive national privacy law. OTI has been beating that drum, along with lots of partners across civil society, for many, many years, and I think one of the things we've emphasized, we do not endorse the Secure Data Act, and we can debate sort of what the right way to do it, but I will say, like, the fundamental understanding, right, that not every cybersecurity problem is a privacy problem, and vice versa, but privacy and security are often two sides of the same coin, and so you can't hack data that isn't collected or retained, right, and you can't, right, so that's a very important sort of simple security maxim, which I think I tried it out a couple of years ago when testifying when APRA had its emergence and there was a hearing on sort of the security data security aspects of thinking through a privacy law and I think. Is a great time, if whether your lens is consumer protection and privacy first, or whether it's data security first, to be reminded of, and to continue to beat the drum. We do need, for a number of sort of people and system security protective reasons, a credible privacy law in this country.

Shane Tews 50:15
Okay? Questions, go ahead to Georgetown. Can you come up here? Just actually, it's hard to hear from the back. Okay, and it's good to see you again. I saw you last week,

Speaker 1 50:34
especially professional and capital capacity perspective, CPO would have capacity process, it's going to be expensive to hire people as well, institutional capacity will evolve that given all of the letters that we are facing. How optimistic are you about the executive orders to deal with issues, or do we need a lot more sort of similar orders into the legislation to get work done?

Shane Tews 51:12
Yes, you're okay. Basically, do we? Is the EO covering the ground that we need for it to right now, or do we need to have more of an actual legislated stronghold on this, okay, yeah,

Kate Charlet 51:25
I mean, I think there's going to be a lot of work ahead in the next 12 to 18 months, and welcome the EO as part of that. I do think that there's reason for optimism in that, you know, medium long term timeframe, but in the 12 to 18 month time frame, we'll be adjusting and adapting, but, but I think as we, as we have worked through that, and that's going to be a hard period of time, but it is nice to kind of see that the technology is there to help take us to the other side of it,

Ari Schwartz 52:01
yeah. I mean, I'd say I totally agree with what Kate said, but I put it, probably put it in slightly stronger words, which is like the short term is sort of unfathomably bad, right? Like, we don't know what's going to happen, and none of it looks very good. The medium term, it starts to say, like, like, okay, you know, now we can sort of see a picture where how to get from the bad to the good, and then that the long term is much better than it was a year ago, right? Because we can actually see a point where we don't, cybersecurity people say, "Oh, we're going to solve cyber security, we're not solving cyber security, because you still have insider threat, you still have all sorts of these things, and AI, other kind of types of AI security issues that you're going to run into, there's there's still going to be cyber security issues, but the random vulnerability and like unpatched thing that just was there, that's that eventually long term looks like it could all go away, which would be pretty good, like we'd have a different cyber security would be different than it is today, and that's that's positive, so if you want to, we want a positive view. Think very, very long term. Yeah,

Prem Trivedi 53:05
I think the other, the other positive view is that nothing galvanizes disparate, divided constituencies like a crisis. And so I think we can, we can not, we can do more than hope, right? We can certainly hope that the sense of emerging crisis, or crisis that is already here, to Ari's point, like we're going to have a really tough short-term period ahead. I think that seems inevitably true, but let's hope that that galvanizes an appropriate response. And not to sort of repeat myself a little bit too much on this subject, but I think it's galvanizing in a way. We talk a lot in tech policy circles about, like, how come how come tech and tech policy never seem like kitchen table politics issues or political issues. Right, I think occasionally they do, but people see kitchen table issues through the lens of what affects them

directly, and rarely are you saying, like, well, I'm worried about my economic security, let me think about tech policy, but I do think that AI, cybersecurity vulnerabilities, and cascading vulnerabilities around systems that are potentially going to touch lots of people's lives in the ordinary course of living and working and playing and going to school and that sort of thing, that's an opportunity to galvanize broader momentum to make progress in areas where, as we've all been talking about, sometimes the human coordination problems are the hardest. So I don't know how to rate the prospects for that optimism playing out, but I think we've all got to be doing what we can to make that more of a reality than not.

Shane Tews 54:21
This has nothing to do with that, your particular question, except for you reminded me. So, when I go out to my dad's other family, is from Denver, and a lot of times my aunt and uncle will be there, and I make them immediately put all of their phones out, and I know that none of them have changed their password or their code since I was last there, and I was like, nope, wait a minute, everybody has to be updated before all, so you, because they just show up with, like, I'm like, you know, tech support showed up, and I'm like, I am not fixing anyone's phone until you update your software, and they don't - they're like, I don't know, it's important to you. I'm like, it's really important, and I actually talk about technology all the time. Lucky you, you have other conversations. I don't know. Thank you. Other questions? Can I

Kate Charlet 54:56
just hand that one thing we haven't said is like, remember. The basics, the basic cyber security, secure by design, password management, two factor authentication, all those things. Low hanging fruit, as relevant as ever.

Shane Tews 55:11
I always say, use two factor authentication. You're just that much harder to get into than the guy who didn't. Yeah, I mean,

Ari Schwartz 55:16
people say, even the people that I'm talking to, they still say identity is the number one issue for vulnerability for exploits that they have in even with this today that might change in the next few months, but it is still will remain important eternally the basics. Yeah,

Shane Tews 55:33
others, you said you might have a question, but were you so good? You don't, don't even have a question. This team, like, yeah. It all right, so then the last question to you all. Summer reading, what are you going to recommend? We've got a lot of paper that Liz worked on, so Aspen Digital.

Liz Chernow 55:53
Yes, okay.

Shane Tews 55:54
And it starts with an R, responsible

Liz Chernow 55:56
advanced access.

Shane Tews 55:58
See, that's beach reading, kids, that's good stuff. All right,

Liz Chernow 56:00
it is speech reading

Shane Tews 56:01
right, Prem. Anything you've got in the works, everybody should be reading

Prem Trivedi 56:06
that we've got in the works. We've done some work recently, a paper that we can, we can share if it's helpful on AI agents. Actually, one of the things we didn't bring up in this, in this conversation too much, although I think Kate mentioned earlier on, is like vulnerabilities raised by the agentic ecosystem and free-flowing data exchanges, there introduces a whole set of vulnerabilities that we shouldn't forget about, even as we're thinking about cybersecurity problems froze by frontier models in certain contexts. So, I can share that paper around, we'll have more building on it to come. But I thought you were asking about what to read in the..

Shane Tews 56:37
I mean, you could.. I actually was no.. but you could have taken any direction, but you went the direction I wanted you to go.

Prem Trivedi 56:41
Yeah, I'll tell you about the novel. She just got off a plane.

Kate Charlet 56:45
I have an on topic and an off topic reading. So, on topic, if you want to learn more about the way in which threat actors are using AI, we have a report on that. We are also just developing a policy paper about ideas for policy makers on how to navigate this moment, but since my red eye was coming back from Santa Barbara and our quantum lab, I do want to just mention we did a blog a little while ago on quantum computing and the timelines around the need to shift systems to post quantum cryptography, so that they are resilient to quantum computers that eventually will be able to break encryption, and the research on that is accelerating timelines and the possibility of quantum computers that are able to break encryption, the number of qubits that are needed to do that are decreasing the hardware, and the error correction in quantum is advancing rapidly. So we recently announced that we were going to migrate to 2029 and I only say this, as you know, if we weren't all consumed by AI and cyber right now, you know, we should also really be thinking about how do we incentivize that preparation for quantum computing 2029 especially when we're talking about, you know, 12 months chaos, like, feels like impossibly long, but it's really not that long, and so we need to think about moving forward on that with urgency.

Prem Trivedi 58:28
Just a strong plus one on that case. Definitely an

Ari Schwartz 58:30
area that we need more investment, as well as move the move to quantum. I will say that one thing that we didn't touch on as much, because we're focused on kind of protecting critical infrastructure. Here is fraud and scams, and like we're looking a lot more into fraud and scams, because internationally it's moved to be like the number one cyber security issue, whereas you know ransomware was number one. Ransomware is still happening all the time, and the bad guys are finding different ways of getting in, and they're using AI to get in as well, but frauds and scams clearly are using a lot more AI, and it's going to get worse, and it's not protecting critical infrastructure, so it's not going to be as, as protected, and it's going to trick a lot of people into turning over money online through frauds and scams, I would look at the reporting that the New York Times did at the beginning of this year on frauds and scams, and China, in particular, China and Burma are the two places where they have these like kind of slave trade that goes on related to putting people into these kind of work. work sites where they are scamming and frauding people from around the world, Europeans and Americans mostly, which seems totally bizarre, but if you, they actually went in and went into the have cameras going into these places, and you can see it yourself, and it's pretty crazy, but that's getting bigger and bigger. Costing more money, people around the world are trying to come up with legislation to stop it. We have an executive order here that has come out. I think it's only going to get to be a bigger, bigger topic, and AI is feeding into it. So,

Shane Tews 1:00:11
Wired magazine does in some really good pieces on that, especially the big butchering situation.

Ari Schwartz 1:00:15
There's actually a bunch of cybersecurity companies have written their own reports on it that are the Wired and the New York Times quote all those, so that's that's those are your sources. Yeah,

Shane Tews 1:00:24
great. Thank you to the panel, you guys have been amazing. Thank you all for being here, and thank you for Tim and Ryan, and all the work that the Internet caucus does. I am absolutely available, all of the people here would love to hear from you, but if you want to learn more, there's something, or there's just because I realize this is a lot. Please feel free to reach out to us, or get a hold of us via Tim, and all the great work he does. So, you guys have a great weekend.