Steptoe

Episode 240: If Paris Calls, should we hang up?

Stewart Baker: [00:00:03] Welcome to Episode 240 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government. Today we're going to be doing an interview with Mieke Eoyang, who's the Vice President for the National Security Program at Third Way and the co-author of a new report that we'll be talking about, "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Fascinating take on the cyber issue and one that has good points and bad. Mieke, welcome.

Mieke Eoyang: [00:00:42] Thank you for having me, Stewart.

Stewart Baker: [00:00:43] It's a pleasure. Also for the News Roundup we're joined by Maury Shenk. Maury is the former managing partner of our London office and advises us on European technology and cybersecurity issues. Maury, great to have you here.

Maury Shenk: [00:00:56] Great to be here, Stewart.

Stewart Baker: [00:00:57] And Dr. Megan Reiss, who's the Senior National Security Fellow at the R Street Institute and many other titles that I'm going to skip over, Megan, because we can't do this all the time. But welcome to the show.

Megan Reiss: [00:01:10] [Laughter] Thanks for having me back.

Stewart Baker: [00:01:11] And Matthew Heiman, who's a Visiting Scholar at the National Security Institute, formerly with the National Security Division at the Justice Department. Matthew?

Matthew Heiman: [00:01:19] Thank you, Stewart. Good to be here.

Stewart Baker: [00:01:22] Yes. It's great to have you. And I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. Why don't we start with Russia? In theory, it's a great idea to sue foreign governments that intrude into American cyberspace and do bad things, and the Democratic National Committee is doing exactly that. They're suing the Russians for having hacked them and embarrassed them on the world stage and maybe cost them the [2016 presidential] election. But the Russians, or at least through their diplomatic service, are starting to make that a little less easy to win, aren't they?

Matthew Heiman: [00:02:04] Yeah, they are. They filed a – you could either call it a letter or a brief – in which they assert as a threshold matter the court doesn't have jurisdiction over the Russian government because they are a sovereign and they enjoy sovereign immunity. And essentially they use the Democratic National Committee's complaint, which appended the unclassified Intelligence Community report on Russian activity in the US related to the 2016 election and Special Counsel Mueller's indictment of various Russian actors. They append that to the DNC complaint, and the Russians very cleverly say, "Ah ha! It seems that you believe these are all directed by the Russian military." Of course, those are sovereign arms of –

Stewart Baker: [00:02:53] "What could be more sovereign than our military?"

Matthew Heiman: [00:02:54] "And if these are military activities, you can't file civil suits against us." And then they go on to state, "And by the way, America does this all the time, and you wouldn't want to get civil suits against you all over the world."

Stewart Baker: [00:03:06] They cite a lot of open-source stuff. Basically there's a not-so-veiled threat that there will be lawsuits against the US government for all the things that NSA does. And they actually take apart the Foreign Sovereign Immunities Act's [FSIA] defenses in moderately persuasive way.

Matthew Heiman: [00:03:26] Yeah. So under that Act there are two broad exceptions that get you out from your sovereign immunity shield. One, you're acting as a commercial actor. So you could imagine if Venezuela, through its CITGO gas stations, were ripping people off or selling them rubbing alcohol instead of petroleum, you might be able to bring a commercial claim against Venezuela. The other one is tort. Obviously –

Stewart Baker: [00:03:54] It's hard to see what the Russians did to the DNC as a commercial activity.

Matthew Heiman: [00:03:59] Right.

Stewart Baker: [00:04:00] I'm not sure how they would have made money unless they had bets on the election. So it's got to be the tort exception.

Matthew Heiman: [00:04:07] And so the Russians' response to that is: "Well, A) no real tort has happened here," and this is the one that I think is kind of the weaker read in their argument which is they say, "We didn't ruin any of the information you have. We didn't take it away. We just made it public!" [Laughter]

Stewart Baker: [00:04:22] "You still have it!" [Laughter] "So we didn't do any damage to you."

Matthew Heiman: [00:04:24] Exactly. "You suffered no harm." But the other argument, which I think is a fairer one, they get down to kind of this venue argument where they say, "Even if you think this is a tort, you've sued us in the Southern District of New York. If anything, your harm happened in DC and Northern Virginia. Wrong venue. Bounce it out of here."

Stewart Baker: [00:04:45] They [the DNC] didn't want to go to DC because there's that kind of dumb Ethiopian decision in which they said, "The whole tort must occur in the United States, and that means if you have somebody in Ethiopia who is planning the tort

or sends the malware to the United States where it does its harm, that that means the whole tort didn't occur in the United States." So they were hoping for a better result from the Second Circuit. So yeah, it does not sound good for this case and maybe not so good for deterring cyberespionage if you're hoping to get countries to sober up about how much cyberespionage they do. I would have loved to have an FSIA exception that allowed you to go at least after people who were stealing commercial secrets for commercial purposes.

Matthew Heiman: [00:05:39] I think that's right. I think the other thing it's a reminder of is that civil litigation is not a panacea for all issues, and it forces you to think even more carefully about how do you effectuate deterrence if civil litigation and public embarrassment is not really an option. And it takes us back to the much more complicated issues of hackback and using cyber weapons. And I know it's much easier to file a complaint, but I think it's just a reminder that there are certain problems, just like a military invasion, that you can't fight with a lawsuit.

Stewart Baker: [00:06:10] There is at least one case that I'm looking forward to more than the DNC case against the Russians, and that's the US case against Julian Assange. Maury, can you tell us how we found out that there's going to be on Assange case?

Maury Shenk: [00:06:28] Well, the US Attorney's office in the Eastern District of Virginia made a filing in a case unrelated to Assange referring to the need to keep the charges against him sealed. It appears that the filing was made completely in error. The other case has some national security dimensions, but it appears that maybe just the same AUSA was working on the two cases and filed it in the wrong place.

Stewart Baker: [00:06:58] Actually, don't you think... My guess is that this is – to find a cyberlaw connection to this case – this was just a cyber mistake. He already had prepared the sealing motion, which is pretty general in the Assange case, and then he got a new case and he said, "Oh, all the law's the same. I'll just change the name." And he forgot to do global replace. He did hunt and replace on the first page or two and

didn't catch all the "Assange"s in the document. And somebody finally read it and said, "Hey, wait a minute." That's what this looks like to me, and that tells me that Assange does have a sealed indictment pending.

Maury Shenk: [00:07:43] Yeah, I think that's right. I mean there's nothing in the public reporting on this that suggests any actual linkage of the case in which it was filed to Assange. So I think it was that kind of user error.

Stewart Baker: [00:07:52] That really has got to hurt. You wonder: What happens when you realize you did that? You want to go down to the court and just sneak all the copies out of the docket or something, but there's no way to do it. If you file something saying I've got a substitute motion, everybody wonders why you did it.

Maury Shenk: [00:08:13] Yeah, that's right. And it's interesting. This is relevant obviously because he's sitting here in the UK. To people here I think there is very little question that if he ever steps out of the embassy here that the UK police are going to be ready to arrest him.

Stewart Baker: [00:08:32] So my impression is the Brits are as sick of him as the Ecuadorians must be.

Maury Shenk: [00:08:36] Yeah. I was thinking about this and wondering what it must be like inside the embassy every day, him getting up, and "Holy [bleep], that guy's still here!"

All: [00:08:48] [Laughter]

Stewart Baker: [00:08:48] Exactly! Yes! It's grim. It's very hard on him. I'm sure. But he can leave any time he wants. It's just that he's going to... He would have been better off coming to United States and taking a four year sentence. He'd be free by now. Yeah, it just goes to show the way the politics of this have played out. If he had not so enthusiastically trashed Hillary Clinton, he'd have defenders on the left. But he doesn't

have any defenders on the left, and he never had defenders on the right. And he's just basically blown any support that might have viewed him as a sympathetic character. And yes, there'll be a few reporters who say, "Well, isn't he a journalist? He just published true facts. He's being prosecuted for true facts." We'll start to hear that once he gets here, but I don't think there's much sympathy for him, and I don't think that's going to get a lot of traction.

Maury Shenk: [00:09:49] Yeah, it's gonna be interesting to see how and when this ends because I think that's basically how it plays out. But the physical dimension of him being in the embassy, when he comes out, whether he decides to take your advice and just face the charges, is a very complex dimension. It could go on for many more years.

Stewart Baker: [00:10:09] Well, frankly I'll be happy to serve popcorn while it goes on because he can move into a British jail for a while as he fights extradition and then come the United States and spend time in our prison system. It's really a world tour for Julian Assange. Okay. Amazon has a new service. If you are murdered, they will protect the privacy of your murderer by demanding that in order to get access to anything that might be on Alexa the government has to go get a court order. Actually, this is a double murder, and the prosecutors have asked for all of the records that Alexa might have. And they had no trouble getting a judicial order. So I actually think this might be less newsworthy than the coverage it got. There was never any doubt that they were going to get an order and no reason for Amazon to do this without some kind of order that would give them legal protection. But it would have been awkward. In other cases they have filed things saying, "We're not going to hand this over because we're protecting the privacy of our users." In this case it was the owner of the device who was murdered along with a second person. So there was nobody that they could take that stand on behalf of other than the murderer. So they quite wisely apparently did not even file. They just said, "Well, we'd like to see the order first." Here's some international cyber news that really doesn't have the United States in it, but 50 countries and companies got together in Paris and signed up to a whole bunch of principles. Megan, what do you think of this “Paris Call,” I guess it's called?

Megan Reiss: [00:12:16] So my take on this is that if you have the major cyber powers not engaging on an international agreement or norms agreement, then it probably doesn't mean all that much.

Stewart Baker: [00:12:33] So this is basically some European countries –

Megan Reiss: [00:12:36] And a bunch of corporations –

Stewart Baker: [00:12:37] Not the Chinese, not the Russians, and of course a bunch of companies who love the idea that they're sitting as some kind of equal alongside the countries. This has of course been Microsoft's view of itself for a long time: "We'll present a Digital Geneva Convention."

Megan Reiss: [00:12:54] Yes.

Stewart Baker: [00:12:55] This is not the Digital Geneva Convention, though. It doesn't look much like what their president was putting forward. Does it?

Megan Reiss: [00:13:01] No, there's a lot of questions that come out of this. And I think one that the cyberlaw community is going to have to grapple with is where do norms in international law actually come from. Can you just say, "This is what we do," and then all of a sudden every country is going to align with it and you're going to be able to enforce international laws?

Stewart Baker: [00:13:22] I'm sure their view is it comes from the same place that regular laws come from: The companies with the biggest budget get the laws that they want.

Megan Reiss: [00:13:30] It reminds me a little bit of the nuke community and a bunch of countries saying, "Okay, we're going to ban all nuclear weapons. We're just not going to include Russia or the US in the conversation," and then hoping that it works. It's a little bit where the US and some of these other countries are going to have to actually agree

to this. And it includes some things that Congress is grappling with. So Congress has been talking about hacking back and what that should actually look like, and this includes a provision that said that we're going to keep companies from hacking back.

Stewart Baker: [00:14:02] That was the one thing I saw in there that I said, "Well, this is dumb." But the rest of it was you know kind of hard to argue with, right?

Megan Reiss: [00:14:08] It's pretty normal. It's mostly stuff that the US already agrees with. I think the non-official response from the US government is something to the extent of: "Well, we're really grappling with what the use of offensive cyber weapons looks like, and maybe we shouldn't sign on to international agreements that we may not actually agree with five years from now." So they don't do it.

Stewart Baker: [00:14:30] So yeah, I suspect there was an NIH element there (not invented here) and maybe not wanting to treat Microsoft as a foreign nation with whom we have to negotiate.

Megan Reiss: [00:14:46] [Laughter] But generally it's not offensive. It's a fine piece of… paper.

Stewart Baker: [00:14:50] Right. Exactly. It's warm porridge. Okay. I sort of agree with you on that. The US and Russia meanwhile have gone to the UN to arm wrestle over their particular warm porridge.

Megan Reiss: [00:15:07] Oh, goodness. Yes. So Russia and the US are trying to present what they called dueling proposals to the UN Committee on Disarmament and International Security, which again is global rules for behavior in cyberspace. And shockingly the US proposal is getting more alignment from Western democracies, and the Russian proposal is getting more alignment from Iran and China. It's shaping out exactly how you would expect this to shape out in every way.

Stewart Baker: [00:15:44] Now presumably these were going to go to the GGE. I guess we call it the Group of [Governmental] Experts. And that effort has already kind of come a cropper once in this administration. Aren't we just setting up another impasse?

Megan Reiss: [00:16:02] I potentially come on the side of I think that any big affirming behavior in cyberspace is going to come through some place like NATO. It's not going to come through a UN that needs to get sign on from Russia and China. It's just not going to happen. So anything that does result is going to be bad actors finally signing on and saying, "Yes, we're going to do that," then ignore it immediately, which actually may reduce the likelihood of developing norms in cyberspace in the end.

Stewart Baker: [00:16:33] Right. Because then people say, "Well, then they're not living up to them, so why should we adhere to these norms that they tried to impose on us?"

Megan Reiss: [00:16:41] Exactly.

Stewart Baker: [00:16:42] Mieke, we're gonna talk to you about a whole bunch of international norms stuff and cooperation stuff, but your report actually doesn't call for any of these grand international bargains. Does it?

Mieke Eoyang: [00:16:58] No it doesn't. I mean we think that norms emerge from state practice, and norms are only as good as their enforcement. So we're focusing on enforcement.

Stewart Baker: [00:17:07] Sounds good to me.

Megan Reiss: [00:17:09] I agree!

Stewart Baker: [00:17:10] Yeah, well, we're all on board.

Megan Reiss: [00:17:12] I want them to be developed. I just think states are going to do it.

Stewart Baker: [00:17:15] Yeah, that's probably right. And they're gonna do it by what they do, not by what they say. Yeah, that's probably right. So everybody has been worried about the Chinese social credit rating. Now there's some indication that they're so proud of it, they're exporting it to Venezuela. Is that right? There was an enormous story suggesting that that's what was going on in Venezuela. If so, it's the only thing that Venezuela has been importing in the last two years.

Megan Reiss: [00:17:46] Well, they've been importing it for a while now. But, yeah. So of course everyone in DC is very concerned about the social credit score, as I think they should be. The potential for human rights abuses associated with it are enormous. And what we're learning is all the predictions that people have been having over the last couple of years that China's authoritarianism and technology link is going to be exported along the Belt Road. Well, we're seeing it in Venezuela. So they're exporting it to like-minded authoritarian regimes. And so you're seeing people coming out concerned that they have a card similar to the social credit score and they're presenting it when they go to the polling booth, for instance.

Stewart Baker: [00:18:32] Or maybe if they just want to get fed.

Megan Reiss: [00:18:35] Yes. And so how could they use this linkage between data and information and use it against civilians if they wanted to? I think if you're a creative authoritarian regime, you can probably think of a few ways to punish people for their behavior.

Stewart Baker: [00:18:52] Yeah, especially if there isn't enough food to go around. Okay. You know it's like this is the week, Mieke, for sweet justice sort of setting up your report. This California guy, who called in a SWATting that left a man dead on his porch, has been flown out to California where he did the SWATting, I guess, and pled guilty, going to jail for 20 years. Cool.

Mieke Eoyang: [00:19:23] Yeah. I mean this is an important reminder that behind these attacks it's not just a faceless army of trolls or some computerized AI that's doing it on its own. There are actual people behind this who should be held accountable for their bad acts.

Stewart Baker: [00:19:36] Yeah, it's great. He's such a jerk. He defended what he did, even after the guy died, by saying, "Well, I didn't kill him." And he's such a jerk that he kind of reminds me of myself when I was 19. You know people are jerks at 19 or 24 or whatever he is. I sort of hope he has a chance to get out in 12 years when he's grown up. But it was a shocking thing. Amazing: They are finally going to rename DHS's cybersecurity administration. And for all the people who've been listening to the show who are sick of hearing about it, this is the last time. The bill has been passed, the House and the Senate. I don't think the president has signed it, but he will. And then the NPPD, which is the National Programs and Protection Directorate, will become the Cyber[security] and Infrastructure Security [Agency]. And we will all know what it does. So that's good news. The Italian police have given up on finding the guy who hacked Hacking Team. Megan, there's more stories about China Telecom-related hijacking of data – this time Google data. Looks like it might be a fake or a mistake.

Megan Reiss: [00:21:01] Maybe, but the question references Google traffic was rerouted through China, and apparently the Nigerians were the problem. I don't know when the big statement is –

Stewart Baker: [00:21:15] They've been told they get the inheritance from the prince if just... [Laughter]

Megan Reiss: [00:21:22] [Laughter] Yes, someone opened spam email. That's what happened. No. I want to know. I want Google to explain more. I think I just don't understand what the repercussions of this are enough: How this could potentially happen, what things could be compromised as a result. There's just so much here, and it's just this like one-off story that "Oh, yeah. By the way, this happened for a couple hours."

Stewart Baker: [00:21:46] Yeah. And it's like the third time we've had a story on this in the last two weeks.

Megan Reiss: [00:21:51] And is this bigger? I mean if I were wanting to do shows of force or showing my capabilities off a little bit, like this is the sort of thing I'd want to do, something that didn't have a long-term impact but showed that someone was capable of doing something interesting. But I don't know.

Stewart Baker: [00:22:10] So I'm more skeptical because I think China Telecom is gonna get hammered over this. They've got 10 points of presence in the United States, and the US has none in China. You know if you're President Trump, the solution is obvious. And I would have thought that they've already gotten subpoenas from the National Security Division saying, "Just what the hell happened here?" That's my guess.

Megan Reiss: [00:22:39] But you do want to know what...

Stewart Baker: [00:22:41] I do want to know. Yes. Because you know the BGP [border gateway protocol] security problems are notorious. And that's what this is taking advantage of, and we need to fix that too. But nothing galvanizes people like an actual abuse.

Matthew Heiman: [00:22:58] It'll be interesting, too, to see if the SEC takes an interest vis-à-vis Google in terms of what sort of risk factors do they have in their disclosures and have they properly disclosed the risks around this BGP traffic.

Stewart Baker: [00:23:10] So here's my guess: Google went through a long and kind of nasty process of NSA-proofing their traffic as a punishment for having a lighthearted smiley face on a PowerPoint slide. So taking their traffic probably gets you very little, if anything.

Matthew Heiman: [00:23:31] I think that's true, but I could imagine an enterprising lawyer somewhere in the bowels of the SEC wondering if there isn't an issue here to pursue.

Stewart Baker: [00:23:41] Okay. Fair enough. And finally, Matthew, does wiping your iPhone constitute obstruction of justice and destruction of evidence?

Matthew Heiman: [00:23:49] Yes, when you're the alleged wheel man for a shooter in a murder and all of the sudden your phone goes blank –

Stewart Baker: [00:23:56] While it's in police custody.

Matthew Heiman: [00:23:57] While the police are asking for it, or yeah, while they have it. So the answer is yes.

Stewart Baker: [00:24:01] Yes. So the only defense there is "Wasn't me. Must be Apple. Tim Cook! Call Tim Cook!"

Matthew Heiman: [00:24:10] Right. Right.

Stewart Baker: [00:24:11] Alright. Okay. Let's turn to our interview. This'll be fun. Mieke is the Vice President for the National Security Program at Third Way. She co-authored a report called "To Catch a Hacker," and it's apparently the first in a series which I'm looking forward to because I kind of enjoyed this. But let me ask you: What's the elevator version of this report?

Mieke Eoyang: [00:24:37] Yeah. So the elevator version of this report is that often in cybersecurity we focus on defense and we focus on the technology. Even when we're talking about hackback we're talking about technological tools. At the end of the day, behind all of these cyberattacks, there's a human being who's making a decision to commit bad acts. And so how do we go after that human? And we looked at the different options that the US government has to go after the human and recognized that

law enforcement is one of those places where it is currently not as focused on this question as we think they should be given the ubiquity of technology and the scope and scale of the attacks that are happening. And many of these are very serious financial crimes. And then we looked at the challenges that law enforcement was facing. We recognized that a lot of the times the bad actor is not in the United States, and law enforcement runs up against bureaucratic hurdles when they're trying to get to people who are in other countries. So it's law enforcement and diplomacy. How do they work together to try and get that bad actor, put bracelets on them, get them away from the keyboard? In order to do that, we wanted to try and measure what the level of activity is on this, and so we went back and looked at all the cyber incidents that are reported to the FBI, measured that against how many law enforcement actions we could find, and –

Stewart Baker: [00:25:50] So this is actually sort of new. Right? Nobody had said, "How are we doing in busting people who commit cybercrimes?"

Mieke Eoyang: [00:25:58] That's right. And we found that out of every thousand cyber incidents, in only three cases are you likely to see an arrest.

Stewart Baker: [00:26:07] So that's not so good. And it's actually worse.

Mieke Eoyang: [00:26:08] That's not so good. It's actually worse because, as the FBI has estimated, only one in six cyber incidents are reported. So on the 15% that are reported, we have 0.3% enforcement rate. So we think with some additional attention to the problem we can help the government be better at identifying these people.

Stewart Baker: [00:26:28] So of those three people that are busted, how many get convicted?

Mieke Eoyang: [00:26:34] Conviction rates are even lower. I'd have to go back and look, but we're talking conviction rates in the single digits. I don't know if your listeners may have seen the Symantec advertisement in the *New York Times*. They talked about

150 arrests. Well, that's great, but then you think that there are 300,000 incidents reported annually to the FBI. Over the denominator, it doesn't look so good.

Stewart Baker: [00:26:56] Okay. So I agree completely with you on this. And the fact is we've gotten so much better at attribution that the things that used to be brick walls now have doors and windows in them that law enforcement can get through. Maybe it's not so easy. Maybe they're 10 feet off the ground, but it's possible to do attribution and to think about law enforcement solutions to this problem. And that strikes me as an advance in the dialogue. We really have not talked enough about finding law enforcement solutions or really what I call "attribution and retribution" solutions, whether it's law enforcement or not. And this report does that. That's all you're focused on. That I think is a really valuable contribution.

Mieke Eoyang: [00:27:47] That's right. We are trying to create another conversation within the cyber debate that is about these questions of law enforcement and what they can do and what we can do to improve them, how we can help them be better at this. Now we've seen things like someone did a survey of cyber incidents that were looked at by cybersecurity researchers to identify who had done it. And even in those cases a very small percentage is actually acted upon by law enforcement. We've heard incidents of companies doing their own attribution, turning that attribution over to law enforcement, and seeing no arrests in those cases where they are giving over names. And so you have to really wonder: What's the capability of law enforcement? What's the priority of law enforcement? Where are the hurdles? We get that this is a very hard problem and that law enforcement may not be able to solve it on its own if people are, say, in hostile foreign countries like this DNC hack where the Russians are claiming sovereign immunity to protect these people. We get that there are some instances that are hard, but just because it's hard doesn't mean we shouldn't be looking for those opportunities to really lift the capability of law enforcement generally.

Stewart Baker: [00:28:56] Yeah, it's hard to believe that local and state law enforcement is ever going to be able to do this. They don't do much of it now, and all of these things are federal crimes. So there is federal authority. Is there really any

expectation that we're going to get state and local authorities up to the point of being able to pursue these cases on a regular basis?

Mieke Eoyang: [00:29:21] I don't know that it makes sense to have them do that given that these are crimes that scale. And so local law enforcement may be seeing something that's happening in a hundred or a thousand other places across the United States. That doesn't mean that there isn't a role for local law enforcement when they get the call from a victim. And what are they doing about helping to preserve evidence, helping to hand that over, helping to feed it into broader statistics so that we can actually draw some of these patterns? There are some serious questions about that and whether or not they're capable of doing that. And then what is the federal government's role in ensuring that they're capable of doing that because so much of this expertise resides at the federal level?

Stewart Baker: [00:29:58] Well, that all makes sense. So I completely agree with you that this is an appropriate place to focus on. It hasn't gotten enough attention. We have more tools than we used to in terms of attribution. But what actually can we do? This is where I think you know your report deserves a lot of praise for focusing on this. I'm less convinced that it has come up with really good policy options for advancing the attribution and retribution tool.

Mieke Eoyang: [00:30:37] That's right. And it's not intended to. This is a foundational document to set out areas for further study for us. So we are not claiming that we are putting forward action-ready policy solutions with this report, and in fact we promised a number of our board members that we wouldn't do that because we feel like there are a lot of areas where we need to do further research to make sure that solutions are implementable by law enforcement, that make sense, and that can be actually used. As a former congressional staffer, I know that often congressional policy recommendations you know are big and bold but have all these hidden consequences. So we wanted to try and think those things through. So yes, it is. A lot of the policy areas that we're talking about are generic and high level. That is intentional.

Stewart Baker: [00:31:25] So your board. Third Way advertises itself as center-left, and it is reminiscent of the '90s and the third way – Blair and Clinton both were third way enthusiasts, although I hope that doesn't poison your fundraising. But who's the board? Is the board people who are funding this? A board of advisers?

Mieke Eoyang: [00:31:52] It's an advisory board because we recognize that solving these problems requires a wide range of policy expertise that we as the staff at Third Way do not have. So we wanted to gather some advisers who have much more in the weeds –

Stewart Baker: [00:32:06] Are those the people that you list at the front of the report?

Mieke Eoyang: [00:32:07] Yes, the people that we list at the front of the report – who have experience in diplomacy, in law enforcement, are computer crimes experts, who are academics, who are congressional experts so that we can have a wide-ranging conversation that brings all of these perspectives into the mix.

Stewart Baker: [00:32:26] Okay. So then let's sort of start exploring. I know you haven't decided what you're going to do, so I'll lobby you on some of this stuff. You say at every turn there are not enough resources. Where do you think you're gonna get those resources?

Mieke Eoyang: [00:32:45] So having spent a lot of time doing earmarks in the defense budget and knowing the difference in magnitude of funding between what is absorbable in law enforcement to make things a priority versus what happens at DOD, we think that actually simply saying, "We need to put more resources to the problem and we need to protect the DOJ resources and FBI resources that are there, we need to protect the state resources that are there, and then look for modest increases," is fine. You know the sort of the appropriations account allocations are made at a higher level. But by calling out these things as priority, we think we'll protect some of those accounts. But I think actually the amounts of money that you would talk about shifting are so small that

DOD would lose them in their couch cushions, and meanwhile DOJ would choke on trying to eat them all.

Stewart Baker: [00:33:38] Well, okay. So it's the usual center-left solution: DOD's our piggy bank, and we could pay for this with a rounding error in the DOD budget. And I'm not going to tell you that's absolutely wrong. Cyber Command is not a sacred cow.

Mieke Eoyang: [00:33:58] I mean we could take it from Space Force. [Laughter]

Stewart Baker: [00:34:01] [Laughter] Yeah, if you could find it. Okay. All that's going to do is you can hire more agents. Right? You can train them better.

Mieke Eoyang: [00:34:14] So it's not just about hiring more agents. So one of the things that we saw that was interesting and we're thinking about this as whether or not this makes sense is that, for example, Secret Service has an attitude that every agent should be cyber capable. Right? That every agent should have some capability in being able to investigate these crimes. FBI does not take that attitude with their agents. And you know in the category of every Marine is a rifleman, if you decide to prioritize certain skill sets and make everyone more capable, then you have a larger workforce to choose from.

Stewart Baker: [00:34:46] I agree with you on that, that that has always been the – Secret Service has prided itself ever since it got into cell phone fraud early on. And you know because it works frequently with financial institutions because of its institutional heritage, it sees a lot of hacking and gets called for a lot of hacking. But you know, to be candid, haven't they just lost the turf battle with the FBI already?

Mieke Eoyang: [00:35:13] No, they actually haven't, and [former FBI] Director Comey testified in front of Congress about the Secret Service's capability in this area. They have a very robust training program. But I happen to think a little interagency competition about this is good for business. It keeps people on their toes.

Stewart Baker: [00:35:27] You would say maybe we should have a system in which we ask each agency, "So show us your stats. Show us that you've actually caught people and busted them, and you will be rewarded at budget time"?

Mieke Eoyang: [00:35:42] Yes. And one of the things that we found interesting in going back and looking at the FBI budget is that they set case targets in every other area of criminal activity of how many they intend to make. And they don't do it in this area. So we don't actually have a good sense of how much it costs the FBI to make one of these cases. We recognize that these are more technologically sophisticated and maybe more difficult and therefore more expensive, but they internally should be able to have some estimate of how much it's going to cost them on average to make these cases and set some targets and let us know how they're gonna do on them. The other thing, and you saw this in the Alexa case we were talking about earlier –

Stewart Baker: [00:36:18] I'll just stop. My experience with law enforcement budgeting approaches is to find something that the budgeteers want and to say, "All of our agents are busy. If you want more of that, you need to give us money for more agents," without ever explaining what their agents are busy on. So it's just a constant kind of ratchet. "What I already have, I'm already using. If you've got priorities, tell me what the priorities are. I'll earmark it for a year or two or three, and then they'll become mine and you'll have to pay me again."

Mieke Eoyang: [00:36:54] So that may be true that that's the sort of budget game that people are playing. But when you're setting basic case targets in other areas like white collar crime and money laundering and all these other things, you can set case targets. You tell us how much you can do, and then congressional folks or political folks or folks at OMB can say, "That's enough or that's not enough, and I want you to raise your targets and I'm going to resource you appropriately for that." But they don't do that. And in fact, what we've seen in looking back at the numbers of the government's own reporting is that they are actually less transparent about what they are doing today than they were five, 10 years ago. When you go back and look at the IC3 [Internet Crime Complaint Center] reports that the FBI used to put out on Internet crime, they used to

have much more granularity about where the bad actors were located and what kinds of incidents these were and what the value of them is. They don't do that anymore.

Stewart Baker: [00:37:47] So John Carlin is not on your board. I've started to read his book. And he said when he wanted to prosecute some state actors, particularly the Chinese, and he went out to US Attorneys, they all said, "I don't have anybody for this. This is you know basically a wild goose chase. You're going to take some of my good people, and they're going to spend two years coming up with an indictment and they won't get to try it." And so it's an enormous resource suck without the advantage of being able to you know do the sack dance when you bust the guy. And isn't that a problem with the stats here too, that these are enormous efforts especially against state actors where you're just not going to get an arrest?

Mieke Eoyang: [00:38:41] Yeah, I think that there are challenges with the state actors, but what we've seen in a number of these incidents, including the Yahoo hack, is sometimes these guys come out to play. And you put a [INTERPOL] Red Notice at them and you can pick them up somewhere else. But that requires you to engage the diplomatic process so that you're working with other governments so when their girlfriend decides that she wants a Mediterranean vacation, you have someone who can pick them up. Right? So we don't do enough of that. That said, there are a huge number of these –

Stewart Baker: [00:39:07] If you are going to do that, you've got to file it under seal. You can't have even one big moment where you announced the indictment.

Mieke Eoyang: [00:39:15] That's right. Then you can announce the arrest, though. But the challenge on these things is they feel – and I'm sure Carlin had this experience – it's not like there is a playbook for these kinds of crimes the same way that we have on money laundering or RICO. And if you start building up a cadre of these cases, and you start rewarding people for taking the risk on these cases and enforcing them by recognizing that these are hard and that people should get promoted for them, then you can think about ways of incentivizing career behavior by saying, "To get to a certain

level, you must have made one of these cases." If you told everybody in the FBI to make SES [Senior Executive Service], you have to make one of these cases, watch the number of changes.

Stewart Baker: [00:39:58] We would get a lot cases.

Mieke Eoyang: [00:39:59] We'd get a lot more cases. And frankly, aside from the state actors, there are a huge number of these cases that are financial crimes that are actual completed crimes where people are losing their retirement savings and their identities and paying huge financial costs, and we are not prosecuting those crimes and we should be prosecuting those crimes. It's one of the few areas where a bad actor outside the United States can do actual harm to an American here in the United States, and we should not consider that acceptable. Law enforcement should be going after those people.

Stewart Baker: [00:40:30] So let me hop on my hobbyhorse on this. If you need resources, the resources are sitting right there. Every company that is at risk of serious cyberattacks, certainly all the financial institutions we were just talking about, has spent boatloads of money, far more than the FBI will ever spend no matter what we do on this. And we have said, “You can spend all that money, but you have to spend it inside your network. Period.” This makes no sense. If you want to free up resources to track people back, to find ways to bust them, you need to go where the resources are, and you need to find ways to responsibly use resources that they would be enthusiastic about using if it meant that they were actually helping the government catch people that were attacking them.

Mieke Eoyang: [00:41:31] So, Stewart, I would be disappointed if you didn't raise hackback. But let me just say then you are encouraging companies to commit a CFAA [Computer Fraud and Abuse Act] violation.

Stewart Baker: [00:41:41] No, no! Of course not. You're not going to tell people to go violate that, but we're talking about...

Mieke Eoyang: [00:41:45] We're talking about essentially vigilante justice. What we have seen in talking to a companies –

Stewart Baker: [00:41:49] Oh, no you're not!

Mieke Eoyang: [00:41:49] What we've seen in talking to companies is they are doing this kind of attribution. They are gift boxing for law enforcement the people who are attacking them. They can do from some of these larger companies by name attribution of the bad guys, and they are not seeing prosecutions on that gift boxing. Law enforcement is the only agency that has the ability to arrest and try those people, no matter how many resources private sector has. They can't. They don't have the authority, and they cannot do that.

Stewart Baker: [00:42:18] So I'm not going to suggest that they should be sending teams to the Ukraine to pick people up, though those would be some of the best-resourced teams for extradition you've ever seen. And I agree with you. If they have gift-wrapped a set of identities, there ought to be a mechanism for identifying such cases and demanding accountability from the law enforcement agencies that they provide it to.

Mieke Eoyang: [00:42:49] I mean, it'd be fairly simple to ask GAO to study how many times private sector has turned over that information to law enforcement and what has happened to those cases. Because if law enforcement is not acting on cases where they have a known suspect, you have to ask why. You have to ask what are the obstacles. And then let's try and figure out how we resolve those obstacles.

Stewart Baker: [00:43:11] So you're not against attribution of attackers by the private sector and handing it over to law enforcement?

Mieke Eoyang: [00:43:21] No, but I don't think it should be uniquely private sector. I do think the government has to invest more in the attribution area because it shouldn't be

that only the companies that can afford to do the attribution of their attackers are the only ones who get justice.

Stewart Baker: [00:43:33] Of course. It would be very – yes. Where they can, we should let them do it rather than saying, "Why don't you wait in line behind the 400 other people who don't have the resources, and we'll get to you in three years." But the idea that you are authorizing, that you are telling people to violate the law is wrong. You can authorize people. The government has the authority under the CFAA to authorize the private sector to provide assistance, so it wouldn't be a violation if it's authorized.

Mieke Eoyang: [00:44:07] So I don't think that we have a problem with authorities here and getting the private sector to attribute. But what we've seen is that they don't see the results from government in spending the money to do that. So why would they invest tremendous resources into the attribution if it is futile?

Stewart Baker: [00:44:23] If they're not going to get a bust out of it and the guy isn't gonna go to jail and stop hacking them.

Mieke Eoyang: [00:44:29] Right. And try and get some recovery for the lost assets. Right? That is the place where law enforcement can do something that no one else can do.

Stewart Baker: [00:44:40] So this is a case for congressional oversight. If that is happening, I'm sure that the people who gift wrap these packages and who complain to you are not going to be complaining quite so loudly if they think that it's going to get him in trouble with the FBI or the Secret Service, but congressional oversight can ask for information on that and they can ask it in an informed way if they get advice from Third Way and others about where to look. And they absolutely should. It's shocking that people would not go after a case that's been presented in that fashion.

Mieke Eoyang: [00:45:15] Yeah. I mean, look, we don't know where the obstacles are and the hurdles are in these cases. Right? This is an important question: Is it that law

enforcement knows who the person is but they can't get to them, or that they don't know who the person is? And depending on which of those two it is, that's in reported cases. There are different solution sets and different policies that you would have to follow to get them to successful prosecutions. That doesn't deal with the large number of companies that never report because they feel like, "Why bother? I'm not going to get any action on this anyway."

Stewart Baker: [00:45:47] But that changes gradually as they see results, as they go to the club and somebody says, "Yeah. Actually, they caught this guy that was hassling me."

Mieke Eoyang: [00:45:57] Exactly.

Stewart Baker: [00:45:58] When you say "law enforcement," it is an odd construction here. You say we need more resources for "law enforcement and diplomacy." What I thought was left out of that, but maybe not, was Treasury. I mean if you're trying to reach somebody who's in another country, especially a country that we don't have the world's best relationship with, you're never gonna get them extradited. So your best bet is to impose sanctions on that person. And that's Treasury's job.

Mieke Eoyang: [00:46:30] Yeah, I think that Treasury has a role to play in this, but I think when we're talking about attribution and we're talking about apprehension, right, those are things where law enforcement and diplomacy play a lead role. And look, State Department has a huge role to play in sanctions as well. We're talking about sanctioning – so Treasury may implement the sanctions, but making decisions about who and where and what the incentives are and what the likely reactions are going to be, part of that is still State Department.

Stewart Baker: [00:46:57] You want the State Department to do that? You think they're staffed for that?

Mieke Eoyang: [00:47:00] Not for the implementation, obviously, but we do mention sanctions in there. When we talk about a carrot-and-stick approach, what we mean is we have to think about where you cannot lay hands on the person but a combination of carrots and sticks. "Sticks" meaning sanctions. "Carrots," right: Can you offer rewards so that people's co-conspirators are going to turn them in? Right? We've done this in the terrorism space. We don't do this as effectively in cyberspace.

Stewart Baker: [00:47:26] That sounds so much like vigilante justice, like you're paying people to hack back.

Mieke Eoyang: [00:47:30] Look, rewards are a time-honored American tradition back to the Old West.

Stewart Baker: [00:47:37] [Laughter] Yeah, so is vigilante justice, but that's alright. Okay. I see that. Let me ask you about the State Department. You've got some kind of an occasional shot, and you've been pretty good about not just saying, "Look, we're so much better than Donald Trump." But there are a few shots at the Trump Administration cutting foreign aid budgets, although I'm not sure the budgets are actually going to go down much, and getting rid of the Chris Painter job of cybersecurity diplomat to the world.

Mieke Eoyang: [00:48:17] We also think that the elimination of the White House cybersecurity coordinator was a problem.

Stewart Baker: [00:48:20] Yes. Right. But I think frankly on these organizational things – do you have a position with this name – those things are given way more importance in Washington than they usually deserve. You can certainly run a pretty aggressive cyber retaliation program without somebody whose job is "cyber czar," and you can do a lot of cyber diplomacy without somebody who is the "cyber ambassador." Can you tell me what it is that Rob Strayer is doing that you think would be done better if he had a different title?

Mieke Eoyang: [00:48:59] Yeah. So I think one of the challenges that we see when we come to cyber diplomacy and specifically on the State Department side is that when you have someone who is below an ambassadorial rank, when they're sitting at the table with their international counterparts, they just don't have the gravitas to be part of the conversation.

Stewart Baker: [00:49:15] Which is pretty ironic because all those people got their ambassadorial rank in order to look like the US ambassador that they were sitting next to in the old days.

Mieke Eoyang: [00:49:23] Be that as it may, there is something about having that rank and as part of the conversation that matters. Now look, could we have effective cross-governmental coordination at the White House level without a formal White House coordinator? Yes. But Stewart, do you really believe that this White House is capable of managing a complicated interagency process to solve this given the disconnect between the president and his own intelligence agencies on other topics?

Stewart Baker: [00:49:51] I hear you. I will return the favor and say: Do you think that having somebody designated as cyber czar would change that?

Mieke Eoyang: [00:49:59] Not in this administration.

Stewart Baker: [00:50:00] There you go.

Mieke Eoyang: [00:50:00] Which is why I think for the first couple of years of this initiative we're really going to focus on congressional oversight. We think it's really important to map the challenges of the terrain, understand what's going on. You can build political will in other places than the White House. And because, as you see in this report, we aren't very specific. This is a long term plan for us to build out a set of comprehensive policies that would be in place for the next president of the United States so that that person perhaps has a different understanding of how the

bureaucracy works, is more able to implement those things, and move towards a much more sort of comprehensive reforms.

Stewart Baker: [00:50:36] Okay. Well, so that means we're going to hear more from you. We're gonna get more reports. We're gonna have more conversations like this. It'll be fun. This will be entertaining indeed. It's always a pleasure, Mieke, to have you on. Are you going to be announcing anything, having any events that people who are listening might want to hear about?

Mieke Eoyang: [00:50:51] I will keep you informed. We don't have any public events currently scheduled, but we will definitely do a series of them over the coming year.

Stewart Baker: [00:50:58] Okay. Thanks to Mieke Eoyang. Thanks also to Maury Shenk, Dr. Megan Reiss, and Matthew Heiman for joining me. This has been Episode 240 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Be sure to send us suggestions for guest interviewees so you can get the highly coveted Cyberlaw Podcast mug, which I am now handing to Mieke.

Mieke Eoyang: [00:51:18] Oh! Thank you.

Stewart Baker: [00:51:19] Yes. There are there are places in Washington where you can actually display that and other places where you might not want to. Send those suggestions to CyberlawPodcast@Steptoe.com. Sometimes I tweet out my ideas for stories, and sometimes I don't. This week I didn't. Sorry. But if you subscribe to @StewartBaker on Twitter, you can see whether I'm swamped by other work or actually focusing on the podcast.

Mieke Eoyang: [00:51:47] And I'm sure Stewart will put the link to our report in the podcast listing.

Stewart Baker: [00:51:50] Absolutely! It'll be in the show notes for sure. And in exchange, Mieke is going to go on the site and rate the show. Give us five stars.

Mieke Eoyang: [00:52:02] I will do that.

Stewart Baker: [00:52:02] That's great. I'm looking forward to it. And you can leave a – it needs to be entertaining, but it doesn't need to be a nice review as long as we get the five stars. And if it's entertaining, I will read it no matter how bad it is. We're going to have Representative Jim Langevin on to talk about his recent work on cyber issues in Congress in the next few weeks. Show credits: Laurie Paul and Christie Jorge are our producers; Doug Pickett is our audio engineer; Michael Beaver is our invaluable intern; I'm Stewart Baker, your occasionally humble and sometimes inquisitive host. That's a reference to a review on iTunes, I think. If you want to know what that's about, you're gonna have to go to the reviews, and while you're filling out one for us, you can read the others. We hope you'll join us next week as we once again provide insights into the latest events in technology, security, privacy, and government.