Steptoe

Episode 236: Twitterlaw and the Khashoggi Killing

Stewart Baker: [00:00:03] Welcome to Episode 236 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking about technology, security, privacy, and government. Today I'm joined by our guest interviewee, who is Chris Krebs, who's currently the Under Secretary for the National Protection and Programs Directorate, but will soon be the Under Secretary [Director] of the Cybersecurity and Infrastructure Security Agency (CISA) – which is a better name and a more accurate name for his responsibilities – at the Department of Homeland Security. Also for the News Roundup, we've got Maury Shenk, who was formerly managing partner of our London office and now advises Steptoe on European technology and cybersecurity issues, and Jamil Jaffer, founder of the National Security Institute and an adjunct professor at George Mason University. I'm Stewart Baker, formerly with NSA and DHS and the host of today's program. Maury, I'd like to kick this off by pulling in what is clearly the story of the week and giving it a cyber connection. The killing of Mr. Khashoggi in the Saudi embassy in Istanbul has brought to light a whole bunch of people defending the Saudi government very aggressively on Twitter and has led Twitter to take down a bunch of bots that it said it had been watching for a while and was just you know slowly taking down. I have my doubts about that, but they clearly have responded to the defense of the crown prince by taking down a bunch of these accounts. And *The New York Times* has written a story about the existence of what amounts to a troll farm in Saudi Arabia of young Saudis who've been paid to defend the regime. Any surprises in here?

Maury Shenk: [00:02:11] No, I don't think there are surprises. I have a lot of friends who are involved in the region, and MBS, as he's called, has done a very good job of public relations, including with our president, convincing some people that he is a

reformer, but he's widely viewed you know as quite a repressive character. And these tactics of hiring – at not bad pay at all – individuals to troll Khashoggi and the like on Twitter and presumably elsewhere is consistent with the behavior of that kind of regime. I just think that... And presumably it could have been known before but just the huge amount of light that is being shown on this as a result of the killing of Khashoggi at the embassy in Turkey is leading to some greater attention to this.

Stewart Baker: [00:03:00] Yeah, I think you're right. I mean this is a regime that traditionally said, "Look, there's enough money to buy off everybody in Saudi Arabia who matters. Let's just spread the wealth around, and then we can take it away if they don't toe the line and that ought to be enough." And for whatever reason – maybe there's not enough money to go around, maybe he's just of a different generation – MBS has reached for some of the standard authoritarian tools, and it now turns out that, yeah, one of the standard authoritarian tools is Twitter troll armies.

Maury Shenk: [00:03:40] Yeah, the Chinese as we've discussed on this podcast before – maybe not just on Twitter but on Chinese and other social media – are really good at this as well. We know the Russians do it. It's a pretty common tool.

Stewart Baker: [00:03:56] Yeah, and this does feel a little more Chinese than Russian in the sense that the people are being paid to repeat a government line to defend the government and maybe to attack regime enemies. But they don't seem to be – maybe there's not enough of them – into the idea of just nuking the whole area of discourse with random trolling. It's a little bit more focused on trying to make sure that the discussion stays within the bounds that the government wants it to stay within.

Maury Shenk: [00:04:32] Yeah, I sort of see it as somewhere between Chinese and Russian. I mean we had that discussion of the Chinese 50 Cent Army, and a lot of them are just spouting positive propaganda about China. I agree with you. This is not quite up to the level of Russian blanket дезинформация [disinformation]. But The New York Times story talked about a lot of very targeted and aggressive trolling of Khashoggi himself, which sounded somewhat more like the Russians.

Stewart Baker: [00:05:00] And Khashoggi was trying to organize a kind of counter-army, a troll army in the West, that would attack the troll army inside Saudi Arabia. So one more thing that got under MBS's skin. Alright. So speaking of controlling the Internet, the EU is, as we all know, pursuing massive and endless competition cases against Google. They've really decided Google is the enemy, and Google is evil in a way that they haven't since they decided that Microsoft was evil. And they've got multiple cases pending against Google and relief against Google. Google just announced that they were going to start charging people who wanted to use the Android operating service. And that one struck me as particularly weird as an outcome from a competition case. You've probably followed this closely, but there's an argument here that I'm seeing in the press that what Europe is trying to do or what the logical outcome of what Europe's doing is to recreate inside Europe the – I won't call an ecosystem but – the vast urban slum that is Android in China.

Maury Shenk: [00:06:28] Well, I think you're right, Stewart, that this is pretty unlikely to be good for the Android ecosystem. But before we talk about that, this weird result, the reason for it is that the European Commission fined Google about $5 billion in July for bundling Android with other applications, and Google is appealing that fine.

Stewart Baker: [00:06:52] Well this is the case where they had to stand on their head to say, "Apple is not competing with Android because Apple doesn't license the iOS, so we want to look at the markets where the operating system is licensed. And what do you know, that turns out to be just Android."

Maury Shenk: [00:07:12] Yeah. So it was a stretch. I agree with you that it's somewhat politically motivated or anti-American perhaps towards Google. So Google is appealing, and rather than you know negotiating with the Commission some looking-forward approach, this is their I think finger-in-the-eye approach or to the Commission as a potential way forward where they've said, "Okay, we will license all our Google Apps besides search and mobile, where we make ad revenue, for up to €40 a phone, although marked down for high-res phones and marked down significantly if you take

Google's search and mobile apps." It's a very complicated deal, and I think they are just trying to show the Commission how messy the logic of the Commission's fine is. That's my guess. Do something that's arguably compliant, but show them it's messy.

Stewart Baker: [00:08:16] This is not unlike their decision to say, "Okay, you want us to pay you for using snippets of your news stories in Google search? How about we don't use them? How would you like that?" And of course nobody liked that, at least none of the people who brought the lawsuit. So maybe that is Google saying, "You know this could get really ugly, and we've got more ways to screw up the ecosystem than you can really tolerate." Fascinating. Okay. Jamil, *The Intercept* has now sent another government employee to prison by publishing their leaks. What's the story there?

Jamil Jaffer: [00:09:02] Well, Stewart, this is the case of Terry Albury who had been a Minnesota FBI agent since 2001. You know Mr. Albury had taken – at least what he's pled to is taking – 25 documents, giving them to *The Intercept*, 16 of which were classified. Apparently the FBI found up to 70 documents on a thumb drive in his house, 50 of which were classified. So obviously you know you can't take classified material and give it to *The Intercept*, even if you are, as Mr. Albury claimed, a whistleblower concerned about racial and religious prejudice at the Minnesota FBI. He was concerned about prejudice against Somali refugees and Iraqi refugees there in the Minnesota Twin Cities area. But at the end of the day, there are protections for whistleblowers in our laws. And you know for those whistleblowers out there who want to take advantage of those, that involves going to your inspectors general. It involves going to your House and Senate Intelligence Committees. It doesn't involve taking classified materials and giving it to *The Intercept*. That will send you to jail like Mr. Albury, who's got four years.

Stewart Baker: [00:10:03] And like Reality Winner, who got five. I did suggest lightheartedly on Twitter that maybe *The Intercept* could borrow the old McDonald's motto: billions and billions served. Well there's at least you know 10 years now will be served by people who were foolish enough to give their stuff to *The Intercept*. The thing I was fascinated by is Albury really used a remarkable amount of tradecraft here. He called stuff up on his screen and then took pictures of the screen. He used encrypted

apps to send the stuff. And he still got caught. I suspect it's because *The Intercept* stories are so long and have so much detail that nobody actually wants to read other than the people who are trying to find the leak that they included some information that allowed the FBI to narrow this down.

Jamil Jaffer: [00:11:06] That is exactly right. And you know obviously that kind of tradecraft demonstrates sort of a knowing behavior.

Stewart Baker: [00:11:14] Yeah, that's right. It made it much harder for him to say, "I'm just an innocent whistleblower." So the other story that I thought was really interesting this week was the Securities and Exchange Commission which flagged email fraud, which is kind of CEO fraud where you pretend to be the CEO and you tell the CFO to pay some invoices or you pretend to be a supplier and you substitute your invoices and your payment instructions for the real supplier's invoices and payment instructions. And the SEC said nine firms lost a $100 million for this, and there could be regulatory implications. Jamil?

Jamil Jaffer: [00:12:02] Certainly true. I mean you know obviously the overall scope of this business email compromise problem – almost $5 billion since 2013 – so a huge amount of capital and money being sucked out of the US economy by these types of compromises. And the SEC is sort of putting people on notice saying, "Look, while we may not have gone after these companies here, it's something that you need to think about in terms of having the right internal accounting practices so that these types of things aren't taken advantage of to extract money from your companies, and we're going to be policing this." And so you know this is an increasing area of concern for companies that the SEC, the variety of regulatory agencies, might get into a more regulatory, more aggressive mode when it comes to cybersecurity protections. So something definitely for businesses to watch out for.

Stewart Baker: [00:12:49] Yeah. So the books and records requirements of the SEC could end up biting people and re-victimizing them after they've paid out these funds. It does suggest that in the long run there's going to be cybersecurity elements to most

people's payment chains of approval. Alright. Maury, there was a very interesting story about China's tech boom, I think in the *Wall Street Journal*, suggesting it looked a lot like a bubble, but the part I was interested in was just how much money from VCs [venture capitalists] in the United States was suddenly pouring into Chinese tech startups.

Maury Shenk: [00:13:35] Yeah, this is one of those amazing Chinese growth stories where Chinese venture capital investment is roughly on par with US venture capital investment now, which is stunning. You know ten years ago, it would have been more than an order of magnitude smaller certainly. And there's a lot of tech development – the world's most valuable private company now is ByteDance. It's a Chinese company. It's worth more than Uber. Particularly some areas do very well in China. A lot of the best AI face recognition companies, because of the Chinese surveillance state, are in China, and these companies are making real money. And there's a huge Chinese government policy to support tech, much more industrial policy than in the US. I know investors who are going into this market, and a lot of money is being made. Yes, it may be a bubble – valuations are crazy – but there's real business there as well.

Stewart Baker: [00:14:32] Yeah, I think there is a lot of opportunity there. What I'm struck by is there was a lot of Chinese money going into Silicon Valley. I think a lot of that is drying up because the US has basically said, "We don't trust this money," and the VCs have responded to that by saying, "Well, if we can't get Chinese VC money here, then we'll take advantage of it by going and investing in companies that the Chinese VCs are supporting in China."

Maury Shenk: [00:15:00] Yeah, well, I think that's right. I think there are questions about the Chinese economy at the moment, but China is seen as a more hospitable environment for tech business, at least globally open tech business, than the US at the moment, which is stunning.

Stewart Baker: [00:15:21] Yeah, that's a surprise. Alright. Well, we are going to finish up with a few quick hits. And Maury since I know you're running out of time, I do want to

ask you about this story from Germany and Austria. It's a long tradition in Germany that of course you know it is only orderly to have your name next to your doorbell in your apartment building, and somebody in Vienna said, "Well, wait a minute. Isn't that a violation of privacy?" And the Vienna privacy officer said, "Yes, it's a violation of privacy law, data protection law," which really bothered the Germans because they were sure that couldn't possibly be right. And even though they are maximalists on data protection, they are also enthusiasts for keeping names on doorbells. So the data protection authorities in Germany have now said, "Oh no, no, it's not a violation of our data protection law." I frankly didn't understand the rationale. I thought they sounded quite unpersuasive when they said that.

Maury Shenk: [00:16:35] No, there's a good reason why this isn't covered by GDPR, which is GDPR only applies to electronic processing and processing in a filing system, and the name on a doorbell is really neither of those. I think there's a very strong argument that the GDPR has nothing to do with this.

Stewart Baker: [00:16:51] Okay. I'll buy that, although what that means is that if you had an electronic system where people's names were displayed electronically, so that you could change it as people moved in and out, that that would be a violation.

Maury Shenk: [00:17:05] Yeah, I think there would be a much stronger argument there, although, as we tell our clients a lot, consent is not the only basis for processing under GDPR. There's legitimate interest, although I suppose if you live in a privacy-protective country like Germany or Austria, maybe there wouldn't be seen to be a legitimate interest in saying who lives in a building. They want their secrecy.

Stewart Baker: [00:17:27] Alright. So the ABA [American Bar Association] has come out with guidance on what the ethical obligation of lawyers might be in the event of a breach disclosure. It's actually – you know this is more or less the second or third time the ABA has looked at cybersecurity and ethical standards. But it's a pretty good analysis. It basically says, "Look, law firms, lawyers have an obligation to keep their clients abreast of any developments in their case, and having their confidential data

breached is a development in their case that they're entitled to know about." And so the rather detailed discussion of data breach is worth looking at if anybody who's listening to this because they're interested in both cyber and law. Good chance you're a lawyer. Good chance you're subject to the ethical obligations of the profession, and there's a good chance that the ABA's analysis is going to be adopted by most of the ethics enforcers around the country. And just to bring everybody up to date: you remember we talked about the Equifax insider trading case where Equifax asked a guy to design a breach notification site but didn't tell him (their worker) that it was for Equifax and he just figured it out and decided since they hadn't told him he didn't have insider information and he could trade on it. And that turned out to be wrong because his job assignment was also insider information. He has now been sentenced to eight months of home confinement and has paid a fine, which means he's basically going to be out twice the amount that he gained from his trading, which sounds like a pretty reasonable and relatively lenient outcome for somebody who was mostly stupid as opposed to venal. And that is our News Roundup for the day. We're going to turn now to Under Secretary Chris Krebs. Alright. Our guest interviewee today is Chris Krebs, who's currently the Under Secretary for the National Protection and Programs Directorate and soon to be Director of the Cybersecurity [and] Infrastructure [Security] Agency – a much better name – at the Department of Homeland Security. Chris, welcome.

Christopher Krebs: [00:20:04] Thanks, Stewart.

Stewart Baker: [00:20:05] So the topic that we have been promising people to talk about is election security.

Christopher Krebs: [00:20:11] Yes.

Stewart Baker: [00:20:11] The election is practically upon us, two weeks away roughly. And there are a lot of ways in which the Russians could have and in some cases did manipulate the election in 2016. How many of them are we better prepared for today?

Christopher Krebs: [00:20:33] Well, let me start by saying this. The best defense against the Russian offense here is vote early.

Stewart Baker: [00:20:40] Okay.

Christopher Krebs: [00:20:41] So if you can vote now, today, whether absentee or in-place early voting, that gives us a better opportunity to detect irregularities. Plus you're able to get in before anything – if anything bad happens, you're able to get in before that time. So vote early. Know what your rights are as a voter. Make sure you know where you're registered. Make sure you know you're registered and the voting precinct. And then know the voter ID requirements, if any, and also the provisional ballot laws as it relates the state where you're registered to vote.

Stewart Baker: [00:21:18] And there the thought is that if there is some sort of problem with voting on election day, people need to be prepared to say, "Okay, I can't vote. I want to vote. I want a provisional ballot, and I want to submit it so that it gets counted once this is all sorted out."

Christopher Krebs: [00:21:36] Yeah, and it's important to note that there are glitches and technical irregularities that happen in every election.

Stewart Baker: [00:21:43] Sure.

Christopher Krebs: [00:21:43] I mean let's be clear here, right? There are IT systems supporting this, and IT systems are not infallible. So just this past primary season in Maryland there was a snafu between the DMV and the State Board of Elections. There wasn't a transfer of voter registration. When people sign up for new driver's licenses, that information didn't go over to the Board of Elections. So folks showed up...

Stewart Baker: [00:22:09] Showed up with a driver's license and said, "I can vote," and they couldn't.

Christopher Krebs: [00:22:13] Yep. You know in their view, they'd done everything right.

Stewart Baker: [00:22:15] Right.

Christopher Krebs: [00:22:17] So what's the process here? Well first and foremost, the election officials have good crisis communications plans in place. They identify the problem, they identify the root problem, they identify the solution, and then they communicate to the voting public. The solution here was show up to vote anyway, and you'll get a provisional ballot. We'll verify everything on the back end, and then that ballot will be counted as cast. Same thing happened in LA County. There was a glitch there earlier this year as well. So these things get caught. You know from a threat model of what a Russian or other actor might do, what we're seeing is actually it would probably be something like what happened in 2016 when the Russians had access to the Illinois voter registration database. Had they manipulated the data to change the poll books or the actual database and someone in Illinois had showed up to vote and their information was deleted...

Stewart Baker: [00:23:11] Then they would have done a provisional ballot.

Christopher Krebs: [00:23:13] Just ask for provisional ballot. Boom.

Stewart Baker: [00:23:15] Yeah.

Christopher Krebs: [00:23:15] It's a measure of resilience in the system.

Stewart Baker: [00:23:17] Yes, and it makes sense that if you just do that, all it will do is delay the final counting of the returns.

Christopher Krebs: [00:23:26] Yep, which brings me to the next thing that I think the American voter needs to be aware of is that: election night reporting? Unofficial results.

Stewart Baker: [00:23:38] Yes.

Christopher Krebs: [00:23:39] You know it's a good indicator, but it's not the truth. You know it's not official results. And in fact certification takes time, weeks even. There has to be a canvass. In some states they audit. So don't necessarily live or die by the unofficial election night [results].

Stewart Baker: [00:23:56] Well, and we all remember Al Gore actually conceded improperly because it turned out things were closer. And my memory is that in 2004, there was a lot of belief that John Kerry had actually won. It never got communicated to the public, but a lot of the commentators were sure that he had it won using those early returns. So yes, it's easy to get it wrong. And *The New York Times* famously said that Hillary Clinton had a 97% chance of being the president. So we have systems in place before we started worrying about this – provisional ballots for the hacking of the voter rolls. Is there any sign that that is being attempted?

Christopher Krebs: [00:24:48] So in 2016 by this point, by mid-to-late October 2016, we had very good intelligence on what the Russians were planning, what they were doing. You know by this point we already knew what was going on in Illinois. We were able to take the indicators out of Illinois and share it across other states. And we saw other communications and targeting scanning...

Stewart Baker: [00:25:09] But they never actually carried anything out in Illinois.

Christopher Krebs: [00:25:12] So Illinois what they did was they went in and they exfiltrated voter registration files. They didn't manipulate. The other piece to be very, very clear about is they did not – we don't have the evidence or any evidence that they had access to vote tabulation machines. That's the real sensitive stuff, and we didn't see it then. We haven't seen anything since then of access to those machines.

Stewart Baker: [00:25:37] So it's quite possible that they did not intend ever to screw with the Illinois...

Christopher Krebs: [00:25:42] I think there's some speculation here for sure that – look, if you back up and you look at what the overarching Russian objectives are, this is not an Intelligence Community Assessment, per se, but I think that it would be safe to say that really they're just trying to get in our heads. They're trying to undermine our confidence in the system itself. Actually getting in and changing a vote? It's actually hard. It doesn't scale well. It's really costly. And the risks are pretty darn high if they do it and they get caught. The specter of being able to do this and mess with the equipment and then getting on social media and saying, "Aha! We were in the systems, and you don't know what we were doing, do you?" That is the risk I think. And so this goes back to kind of the top of the show: get out and vote. That is the best way to push back on these Russian efforts to get in our heads. It's vote. Don't let them discourage you from voting.

Stewart Baker: [00:26:47] Right. So that makes sense, and I agree with you. It's kind of getting in our heads, and to get into our heads they more or less have to admit they did it, which they've been doing a lot of advertently and inadvertently lately. So the other kinds of things that the Russians did in 2016: they hacked a lot of campaign and individuals and then released the information so that it would have an impact on the campaign. We certainly haven't seen any releases from WikiLeaks and DCLeaks and Guccifer 2.0. They've all been silent, partly because there's no national campaign. What is the department able to do about preventing that kind of hacking?

Christopher Krebs: [00:27:37] So again you know defense here. Prevention is key. We've been working with the RNC and the DNC and the state-level party heads, party chairs on: basic training; basic awareness; recommendations issued; partnered with the Belfer Center and pushed out some campaign security checklists. But you know this is one of those things where we can give a list of 15 things that campaigns that are on shoestring budgets just don't have the talent, the wherewithal, or the cash to pay for it. So you know what we've seen is a lot of the cybersecurity companies and the IT companies offering free services, which I think is a great move forward. But even just the basics of you know enable multifactor authentication just make it that much harder

for the bad guys to get in and get to that sensitive information. And that's probably priority step number one. And just you know again be mindful of what you're pushing around via email and use *The Washington Post* test, right?

Stewart Baker: [00:28:38] Right. How would you like to see this on the front page of *The Washington Post*? Although I continue to love the [French President Emmanuel] Macron approach, which is: put in some things that are shocking headline generators that you know you can disprove and wait for them to steal it and try to get you. It's risky, but it certainly worked for him.

Christopher Krebs: [00:28:59] It's a counter-counter information operation. Yeah.

Stewart Baker: [00:29:02] So here's a question not in your area of expertise, but if I'm a security firm and I want to offer cybersecurity capabilities to the campaigns, is there a risk that that will be treated as an in-kind campaign contribution, or have you addressed that?

Christopher Krebs: [00:29:21] We're rapidly getting out of my skill set and safe zone, very narrow as it is. So a couple of companies have done this, and they've asked for exceptions from the Federal Elections Commission. They've been granted those exceptions. So we're seeing a recognition of the challenges here and that we can't play this game with two hands or one hand tied behind our back. And you know this is '18, the midterms. They think 2020 is the big game probably. So as we kind of go through this process in advance and we do some after action reporting after November 6, we'll find out how to probably streamline this process. The companies will, and the FEC will. And my hope is once we get through that process, we can do a better coordination, because one thing I am seeing with a lot of these companies that are offering free services is the election officials down range are being inundated and they can't really kind of contextualize this service vice that service. What does it get them? So we need a more coordinated almost holistic approach. But that's tough. But if it's free and presumably not a loss-leader free, then there's probably a better way we can do this.

And so we can use some of our coordinating mechanisms through DHS and the critical infrastructure partnerships I think to figure out what this suite of services looks like.

Stewart Baker: [00:30:51] I would have thought that three-quarters of it would be: use Gmail or Hotmail and turn on two-factor authentication for your email accounts. And you're at least 60% of the way there.

Christopher Krebs: [00:31:03] Yeah, for campaigns for sure. But there's also DDoS and DDoS protection and mitigation. I mean those are the kind of cheap threat models that we're looking to overcome.

Stewart Baker: [00:31:15] So 2018, from your body language at least, is not looking like it's going to be a debacle, not even looking like it's going to be a repeat of 2016. I realize you're...

Christopher Krebs: [00:31:27] I will never say that.

Stewart Baker: [00:31:29] [Laughter] I didn't expect you to. But let's assume that that's the case, that it goes pretty well. Do we treat 2018 as our opportunity to have a really good intramural game while preparing for the varsity game in 2020?

Christopher Krebs: [00:31:49] So you know our baseline planning factor right now is kind of what the Russians did in '16, how they were conducting spear phishing campaigns, trying to get access to voter registration databases, things like that. And then we're looking: okay, if we know anything about the Russians – I've said this a bunch lately – if we know anything about the Russians, it's when they come back, they're always a little bit better or they're a little bit different. So how would they improve or how would they mix up their approach? So even though we haven't seen anything right now, we're still preparing as if they're coming back and thinking a little bit more creatively about: okay, we only have two weeks 'til game day. What could they do in that two-week period to mix things up? and whether it's a very small-scale targeted technical attack on an election system somewhere out there and then amplification through social

media, that's kind of where we're gaming it out, trying to get ahead of it. So again we're just hitting right now really hard the best practices: password resets, you know spear phishing awareness campaigns, heightened level of awareness. Now running up into 2020, I think that is for sure where – you know because more is at stake, right? We are going to also, given the presidential race, probably see – and the time to build up and learn more from Russian activities – look for more countries to probably join the game.

Stewart Baker: [00:33:21] Aren't we seeing some indication of Iranian interests in this field? Maybe that's on social media rather than actually doing the hacking.

Christopher Krebs: [00:33:30] So you know if you look at the Intelligence Community Assessment (January 2017), you know there are a range of activities that the Russians used or took up. You know there's the technical attacks against election systems, there's the hack-and-leak that you talked about, and then there's just the broader information operations. And on that right side of the spectrum, the information operation, we see a whole range of countries in the influence space. Iran...

Stewart Baker: [00:34:03] There was a story today about Saudi influence.

Christopher Krebs: [00:34:06] Yeah. Look, I think this is just kind of the new normal in terms of how countries are using information operations and using the information economy almost in militarizing it – or "weaponizing" is probably the better way to put it. So we'll continue to see this sort of activity going forward. Really the question I think we have to ask is how do we harden or build the resilience of the American people to be able to withstand this sort of stuff within the framework of the First Amendment and our you know privacy and civil liberties principles? So that's the real hard thing right now that we're trying to work through.

Stewart Baker: [00:34:48] So I would have said when it comes to hacking the voter rolls or hacking voting machines or even hack-and-leak that DHS pretty much has the lead. Who has the lead on dealing with the resilience of the American people to these sorts of divisive and manipulative Twitter and social media campaigns?

Christopher Krebs: [00:35:17] So on the countering foreign interference, countering foreign information bucket, I'll call it, the FBI has lead for the mitigation and the disruption. In terms of the resilience building and awareness building, that's a DHS-FBI kind of shoulder-to-shoulder approach. We pushed out – the FBI took lead, we supported – the Protected Voices campaign, which was about how to protect yourself, how to protect your campaigns. And then we're working through a number of public statements and other campaigns to increase awareness. And you know great example: the 2017 Intelligence Community Assessment is just a gold mine of activity and information about what Russia specifically but broader nation states might do. Look at kind of the static elements of the ICA – and what I mean by static is the things that are day-to-day, they're always there – it's the same mouthpiece and specifically RT and *Sputnik*. State-sponsored media. They are the mouthpiece for the Kremlin. They're still there. In fact they're registered under FARA [Foreign Agents Registration Act] here.

Stewart Baker: [00:36:31] About time.

Christopher Krebs: [00:36:31] So we need to call it like we see it and say this is...

Stewart Baker: [00:36:35] This is the Russian government line.

Christopher Krebs: [00:36:37] Yeah. It's in their charter. It's in RT's charter that they will carry out the message of the Kremlin overseas. So that is part of this awareness campaign, and you know letting the American public know if you see anything from *Sputnik* or RT, know where it's coming from. Validate from another source. This is no different from the '70s and '80s in *Pravda*. It's the exact same thing, in fact. So it's a reminder, I think, because we forgot maybe that there are nation state peers and adversaries out there in the counterterrorism era.

Stewart Baker: [00:37:12] Plus the line that they're pushing is very different from the Communist International. Now it's a much more nationalist line which people didn't associate with the Soviets. And so no one has had to worry about making sure that they

aren't too close to the Kremlin line when they talk about you know whether the United States should be part of NAFTA or USMCA [United States–Mexico–Canada Agreement].

Christopher Krebs: [00:37:41] But I mean you made the point best I think earlier. They're trying to undermine our system, our system of government, and our faith in our democracy. That is their objective.

Stewart Baker: [00:37:50] And we are at a disadvantage – or at least the government is – because even RT has First Amendment rights.

Christopher Krebs: [00:37:59] Yep.

Stewart Baker: [00:38:06] Okay. I said at the top of the show that you're going to get a new title.

Christopher Krebs: [00:38:10] From your lips to God's ears.

Stewart Baker: [00:38:10] That's passed both houses, right?

Christopher Krebs: [00:38:16] So it passed the House last December. And then went over to the Senate and passed out of the Senate two or three weeks ago. But due to a small technical change – there was a savings clause introduced at the behest of another committee –so it goes back over to the House. But from my understanding, the conversations are that we should be in good shape. And it's just a...

Stewart Baker: [00:38:41] Just a matter of finding a time and a place to get it through.

Christopher Krebs: [00:38:44] Yeah, and you know unfortunately the House comes back the week after the midterms for four days – or three, even, because Monday is Veterans Day, so the come back on the 13th. And then the following week is Thanksgiving. So you know clock's ticking. There ain't much time left.

Stewart Baker: [00:39:00] Oh, dear. Well, it would be a shame. DHS has done very well over the last few years implementing changes and then asking Congress to ratify them. That's the only legislation that DHS has gotten. And this is another thing where you'd say, "Well, we already do this. This is kind of what our job is. Why don't you just ratify it?" And that is less controversial than asking for something new.

Christopher Krebs: [00:39:25] Yeah. You know this goes back to the good old days of DHS 10 years ago when after 2SR (Second Stage Review) [Initiative] and some of the other things that you were a key player in, and Congress through the appropriations process clamped down on the [Section] 872 [of the Homeland Security Act of 2002] ability to do the own reorg. So I am in a unique position in that we are in a unique position where all I'm asking for really is a name change and a streamlining for the organization, and that's it. We're not creating anything new here. It's elevating an existing set of authorities and organization and appropriations and all that good stuff. Other departments have over the last year stood up entirely new programs and then asked for congressional authority or approval. So we're in a weird place, but we're trying to do this right. We're trying to do this through consensus building. This goes back you know. Under Secretary [Rand] Beers back in the early years of the Obama Administration really teed this up, but I think just after you know a good campaign – I've gotta admit – we've hit this pretty hard. And you know also the fact that industry really came on board this time. I think they understand...

Stewart Baker: [00:40:43] So that is a difference, and some of the credit goes to you. Industry used to say, "DHS cybersecurity? Oh, no. No. I'm sorry. They can't do anything." And you don't hear that anymore, or at least I don't.

Christopher Krebs: [00:40:58] You don't hear it as much as you necessarily used to.

Stewart Baker: [00:40:59] Right. And the people you hear it from don't know that much. They're repeating stuff they heard 10 years ago. It does seem to me that DHS no longer

has a reputation for not really knowing that much or being able to do that much on cybersecurity.

Christopher Krebs: [00:41:13] But you know it's not like I came into this role and snapped my fingers and things changed. The prior team under Suzanne Spaulding did a great job of building a sound foundation, making the right budget priorities. But we have a long, long way to go. I mean you know DHS, the cyber budget – my cyber budget at DHS – being one of the five mission areas is 1% of the Department's budget. It's actually less than 1%. But you know who's squabbling over quarters in the sofa cushions? We have a long way to go, I think. But in part because the threat landscape has evolved so rapidly and it continues to shift and change and it's – you we need to be much more nimble as government. We need to be much more agile in our procurement processes, but at the same time we need to look at industry and say, "Alright. Let's be clear. Industry, you guys are always going to be faster than us, always have probably better tooling. What do we have that is uniquely governmental?" In part that's intelligence, infusion of intelligence with open-source information. But the other piece is the ability to you know not be committed to profit centers and that I can look for market failures whether within sectors or across sectors and if there's no business model for it, doesn't matter. I can do that. There's a value in it.

Stewart Baker: [00:42:38] Elections would be a good example because the secretary of state budgets for elections are tiny.

Christopher Krebs: [00:42:47] Right. But the key – and this is what I've really hit hard on – is that what we do at NPPD – and hopefully CISA soon – is going to be stakeholder informed and based on values. So everything I do should be, for the most part 90%, driven by what stakeholders need from me. We'll align capabilities against that requirement base. And then we have to deliver value. Now we are able to share threat information and we can do other things based on threat information, but I think part of what you're hearing from industry right now is that we are taking a prioritized risk management approach to solving a pretty thorny problem. Now it's early. The returns are still pretty small, but you know from small things grow big things.

Stewart Baker: [00:43:43] So one of the things that I would have thought that industry would be interested in is DHS playing a role that moderates and coordinates all the regulatory agencies, all of whom now believe that cybersecurity is an important part of their mission, and they may have come aboard late but they have authority to regulate. And the question is are they going to use that authority to regulate to start splintering the effort and demanding things that sound good but aren't crucial to security or just ask for things that made headlines in their industry. And DHS has an ability to say, "These are the things that are most important. You need to focus on those." And I would have thought that industry from time to time would want to, be able to come to DHS and say, "My regulator doesn't understand this."

Christopher Krebs: [00:44:39] So I think you touch on an important part, and it was a key element of Executive Order 13636 back in 2014. Regulatory harmonization. Do we have the regulatory authorities we need for cybersecurity, and where we do have it, are we focused appropriately? And the returns from those discussions in the last administration were like, "Yeah, yeah. We're good." Everything's I think appropriately tailored, and it probably was at the time. There are challenges working with independent regulators. The independent agencies don't necessarily have to listen to whether it's the White House...

Stewart Baker: [00:45:17] Frankly, they should have to. This is national security. They don't get to say, "Oh, but I have my own constituents."

Christopher Krebs: [00:45:23] So I think we – Senator Heitkamp mentioned when I was going through the confirmation process, she said, "I hope you have sharp elbows." And I think this is one of those areas where we need to be a little bit – not a little bit better, but a lot – better coordinated. And I think it's in part up to my agency working with NIST [National Institute of Standards and Technology] and others to say, "Look, here's the baseline. These are the things that we just have to do." A lot of the area for improvement that I see is education and awareness. I know people are going to hear that and roll their eyes like, "Ugh, enough awareness and education." But you know

even when we talk about SEC and their examiners, I need to do a better job of engaging the examiners and educating them on my capabilities and my team's ability so that when they go out to the field and they meet with their stakeholders, they can say, "Look, you've got a problem here. Here's who you can work with at DHS to go address that issue." And so there are opportunities for engagement excellence as I see it all across the interagency.

Stewart Baker: [00:46:28] Absolutely. And you just did an MOU [memorandum of understanding] with the FDA. And it always struck me as I watched that to some degree that it was perfectly clear that the FDA was desperately dependent on DHS and the ICS-CERT [Industrial Control Systems Cyber Emergency Response Team] for an understanding of the risks of implants. And it's sort of nice to see them not insisting on their autonomy on this but wanting to work with you on serious security issues.

Christopher Krebs: [00:46:58] I think part of this – so it's funny the relationship with FDA. We've always had a really good technical relationship with FDA, but at the leadership levels… Just last hurricane season working through some of the Puerto Rico issues in the pharmaceutical manufacturing base down there developed a pretty close relationship with Commissioner Gottlieb. And so as we say, "Hey, how do we build on this partnership? What can we do next?" One of his areas of interest was cybersecurity said, "Alright. Let's go see how we can collaborate," and the fruits of that relationship are bearing fruit right now.

Stewart Baker: [00:47:32] Well, congratulations because it couldn't be worse than when I was there. I wanted to make sure that everybody had antibiotics and an emergency kit of antibiotics in the event of an anthrax attack. And the FDA said, "You can't give that out without a prescription from a doctor. And if you tell people they should go out and get it without a prescription, that's a felony and we could have you indicted." They didn't quite say they would have me indicted, but they came close. So if you pick the wrong side, they can be very prickly indeed. So let me ask, in closing because I know you've got another child on the way, number five – this is terrific – and heading off

to a doctor's appointment: what's coming up that DHS is going to do either on elections or more broadly on cybersecurity issues that listeners should be watching for?

Christopher Krebs: [00:48:28] So I think the president's National Cyber Strategy gives a pretty good outlook on where we're going in terms of both federal cybersecurity – so we do see opportunities for greater centralization of services. My team will be providing SOC as a service (security operation center as a service), instant response capabilities, but also really bottoming out on what agencies are responsible for and where they can look to DHS for additional help. So that's federal. On the critical infrastructure space, really moving into supply chain. So the *Bloomberg* article from a couple of weeks ago? Fascinating stuff.

Stewart Baker: [00:49:05] Yes. I think you've said you haven't seen any validation.

Christopher Krebs: [00:49:11] And even as recently as last week, DNI [Director of National Intelligence] Coats was out there and again speaking to the issue. But it's not the veracity of the story...

Stewart Baker: [00:49:18] But the plausibility is high!

Christopher Krebs: [00:49:18] It's the plausibility. Yeah, and this is an area that – I look at this as probably the greatest opportunity space across the federal government right now in terms of supply chain security. You know the MITRE "Deliver Uncompromised" report is just a great piece of work. And there needs to be a lot. The federal government, through the procurement process, has an incredible amount of leverage, and we need to figure out how to optimize that leverage to get better security down through the system, whether it's in the defense industrial base or just the broader ICT [information and communications technology] supply chain.

Stewart Baker: [00:49:56] Or you know just our weapons system, as a recent GAO report suggested we have a real problem there.

Christopher Krebs: [00:50:02] So supply chain and industrial control systems, and you know you take it down the next level, it's Internet of Things. Look, the attack surface area is exploding in front of our very eyes – exploding in a figurative way, not a literal, of course – but you know there's a lot of room for DHS to provide value into the market.

Stewart Baker: [00:50:28] Sounds good. I'm very excited. From the little beginnings that we had in 2007-2008, there's been a consistent pattern through the Obama Administration into the Trump Administration of DHS taking on more and doing more. And you're part of that tradition. Chris Krebs, thank you very much for joining us.

Christopher Krebs: [00:50:50] Thank you, Stewart.

Stewart Baker: [00:50:51] Okay. Thanks to Maury Shenk and Jamil Jaffer as well for joining me. This has been Episode 236 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Don't forget to send us suggestions for guest interviewees. We'll give you a highly coveted Cyberlaw Podcast mug – value less than $20. Chris, I'll give you one, if you can accept it. And send the suggestions to CyberlawPodcast@Steptoe.com. I have started posting the stories I think we'll cover in the week on Twitter, @StewartBaker, so you can look for them there. Be sure to rate the show. I have just discovered that we actually have two different instantiations of the show that Apple has recognized, and they have different reviews and different ratings. So please go in and rate them both. I have now found a few entertainingly abusive reviews, so I will be reading those sometime in the next couple of shows. And tune in. We have a panel coming up of CISOs, including the deputy CISO of DHS. And I'm going to have a conversation with Dipayan Ghosh, who's the co-author of a report on digital deceit and the efforts that foreign governments and sometimes domestic players have made to shape our national conversation in unhappy ways and what he thinks should be done about it. Laurie Paul and Christie Jorge are our producers. Doug Pickett is our audio engineer. Michael Beaver is our intern. I'm Stewart Baker, your host. Please join us again next time as we once again provide insights into the latest events in technology, security, privacy, and government.