Steptoe

Episode 246: Russia's Successful Search for Deterrence on the Cheap

Matthew Heiman: [00:00:06] [Music] The other part of the story that I just love, Stewart, is the fact that El Chapo had him put a microphone eavesdropping feature on 50 phones so that if you had a conversation with El Chapo, whether you were his girlfriend or one of his deputies pushing drugs, when you hung up and maybe after the boss or boyfriend chewed you out, you said, "Boy, that guy's a real jerk," El Chapo knew. If you're working for an insecure boss that has cartel-like tendencies, just think about that after you hang up. You may still be effectively on the line with your boss.

Nick Weaver: [00:00:34] Especially if the boss gave you the phone.

Stewart Baker: [00:00:37] Yes, exactly. Yeah, that's the problem. On the other hand, you know look, everybody who works for government, their boss gave them the phone, and there's a notoriously insecure guy at the top of the government. So you never know. I think those White House secure phones may look more like El Chapo's than you think. [Music] Welcome to Episode 246 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government – in the middle of a government shutdown, plus a six inch snowstorm that would have collapsed the government anyway, so we all have plenty of time to talk about cyberlaw. I'm joined by: Maury Shenk, who was in our London office and now advises us on European and Asian technology and security issues; Matthew Heiman, who is a visiting scholar at the National Security Institute, formerly with the National Security Division at the Justice Department; Nick Weaver, a senior researcher at Berkeley, also a lecturer there. And I'm Stewart Baker, formerly with NSA and DHS, the host of today's program. We're gonna jump right in because I really want to talk

about this story – I think it's in the *Wall Street Journal* – about what the Russians have been doing in our power grid. Matthew, get us started.

Matthew Heiman: [00:02:04] Well, the story says that the Russians have been lurking in our power grid for quite some time, and their most common way of accessing it is not to go through the major utilities, which have some semblance of cybersecurity, but it's to go through the endless number of contractors that support these utilities, then working their way through them. They get passwords. They phish. They do all of the things that hackers normally do to wreak havoc. And then once they're in the system, they're there, and they have done a pretty decent job up until now of remaining dormant and undetected.

Stewart Baker: [00:02:36] So, Nick, it looks as though one of the ways they have found to get in is to figure out websites, obscure newsletter websites, that might be visited by people who care about power grid technology and to poison the website so everybody who goes there ends up owned and then to take their ownership from there to the next level and on into the grid. Is that pretty much what they're doing?

Nick Weaver: [00:03:03] It's a good summary. So they are starting with what we call "watering hole" attacks, where you compromise a website, use it to either get passwords or inject malicious code directly onto victims. From Victim A, then you send out mail to Victim B, that if the victim acts on would be triggered. And because it's people you trust, you're going to say yes, because let's face it, Stewart, how many people you know send you things like PowerPoint attachments or links to Dropbox or Google Docs? It's simply we've created this workflow around trust that makes it very easy to do certain things, including if an attacker takes over your account, to be able to attack your colleagues.

Stewart Baker: [00:03:50] Well, and in some of these cases, I think people were a little suspicious, and they sent notes back saying, "Is this really you?" and the hacker said, "Yes, yes! It's me! Open the attachment!"

Nick Weaver: [00:04:01] Yeah. What would you do if you were controlling somebody's email account and you got a request back that said, "Are you sure this is you?" You'd say, "Yeah, of course it's me."

Stewart Baker: [00:04:11] Well, okay. But in many ways this is very ballsy, not only sitting on the account and sending out fake reassurances, but the fact they must have known they were going to get caught doing this. And isn't this kind of Vladimir Putin's thumb in the eye of what was then the Obama Administration is now the Trump Administration?

Nick Weaver: [00:04:34] Yeah. But the Russians have been pretty brazen now for a few years, and what consequences have they suffered? We haven't really upped sanctions. We haven't done the option of really getting them off of SWIFT [Society for Worldwide Interbank Financial Telecommunication network] and getting them out of the global economy. We just take it.

Stewart Baker: [00:04:57] Well, Matthew, let me ask you: This really raises the question because this is basically Putin saying, "If I don't like what your administration does, I can take out power in large chunks of the country for an indeterminate amount of time, causing you endless pain – maybe causing deaths – and dramatically shrinking your political capital." He didn't have to say it because we all know it now that he's gotten into these systems. What is the right response to that? Do we have to wait until he actually turns out the lights?

Matthew Heiman: [00:05:33] Well, I certainly hope not because that would seem to be a bit like the old saying of closing the barn door after the cow leaves. You know I think there are things – and I'm hoping you know as we read these stories in the *Wall Street Journal*, I certainly hope to the extent the Russians are mapping out our grid, that our Intelligence Community is doing the exact same thing. I hope they're being a little bit lower key about it. But I also think we've got to start thinking about optionality so that when these things happen, maybe we send a couple of shots across the bow via cyber means to say there is a consequence to this. So maybe the lights start flickering in

some far-flung town in Russia because I think until we do that, as Nick just said, Putin in his mind, it's a green light and there's no consequence to doing it.

Stewart Baker: [00:06:18] Yeah. My favorite idea in this area is to say, "Dear Vlad, we know you're in our grid. We understand the implicit threat. We're trusting in your responsibility not to use the tools that you have given yourself. Similarly, we have put a whole bunch of mines at the bottom of all your harbors, but don't worry! They're at the bottom. They won't come up unless they get a signal from a device that we tied to the grid, and as long as the grid stays up, they stay down."

Nick Weaver: [00:06:45] The other thing that we should worry about is the oil refining infrastructure because a computer attacker in an oil refinery, in particular, who's good could make it go boom.

Stewart Baker: [00:06:58] Yes, absolutely could. We haven't seen that, but we've seen attempts to do that in the Middle East, probably Iranian-inspired so maybe they weren't quite as good. I think the Russians are better and probably could pull it off. They certainly could brick all the machines in a refinery and cause the refinery to have to shut down. That's the cheery news for the week. In some actual good news, Maury, the "right to be forgotten" lawsuit has gone to the European Court of Justice, and the question is: Should we give Americans the benefit of our European censorship? In other words, if Google is told to take down a reference to some European who doesn't like the news story about them, should Google be required to take it down everywhere in the world? And Google says no. The French data protection authorities say yes. And there was just some preliminary good news in that litigation.

Maury Shenk: [00:07:56] Yes. One of the Advocate Generals of the European Court of Justice, Maciej Szpunar – I'm hoping I'm pronouncing his name correctly.

Stewart Baker: [00:08:05] Actually I checked. That's a perfectly legitimate pronunciation.

Maury Shenk: [00:08:09] Thanks. I got lucky. And so he has agreed with Google's approach. Google's approach is if there is a successful right to be forgotten request, they block it throughout the EU, and they block it from abroad when one of their foreign sites (non-EU sites) is accessed by a person from the country where the initial complaint came from, so not anybody in the EU. And the ECJ Advocate General has basically backed that approach. His rationale was effectively if we take CNIL [Commission Nationale de l'Informatique et des Liberté], the French data protection regulator's approach, we're gonna have a global race to the bottom on free expression. You can imagine that Turkey adopts a similar policy and says any anti-Erdogan website must be blocked globally and any number of other similar examples, and it's refreshing to see that the Advocate General has not gone for that.

Stewart Baker: [00:09:03] Yeah, it is a surprise. I continue to believe that this European Court of Justice is so profoundly anti-American that any opportunity to beat a US technology company over the head, they will want to seize. So I don't know that they'll take the Advocate General's advice, though they usually do. But it's nice to see a certain amount of sobriety from European regulators on this.

Maury Shenk: [00:09:30] A word of caution: The Advocate General, they usually take his advice, but the Google Spain, the original right to be forgotten case, was one of the ones where they didn't. [*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014)]

Stewart Baker: [00:09:39] Yeah, because they hated Google so much they just couldn't resist. That's true. And you know they've written opinions based on erroneous newspaper clippings because they didn't want to send the case back for actual findings of fact because that might have gotten in the way of their ability to punish Facebook, I think it was in that case. They're just deranged by not even Trump, but they're deranged by the United States. This Week in Drone Law: The UK has been suffering through a nightmare that DHS and the FAA originally foresaw in the United States and asked for legislation to address. Maury, can you tell us what was happening in the UK, and then we'll ask Nick about the US legislation?

Maury Shenk: [00:10:29] Yeah. I mean it was really big news here. There was just before Christmas, drones kept popping up near Gatwick Airport, and they'd try to find it, try to find where it was being controlled from. It would disappear, and it would pop up again. And these were small drones, probably wouldn't have damaged an aircraft, but they weren't willing to take the risk and they shut down Gatwick for a couple of days. Hundreds of thousands of people were delayed in their travel. My wife's parents live near there. We were headed there, and it even affected the traffic, even if you weren't going to the airport. You know and there's no easy solution. Apparently the military is allowed to shoot these things down, but then you've got to worry about where the bullets that are shot at it will land, where the drone is going to land. Bruce Schneier has an interesting piece on all the risks of this. There just is not an easy solution.

Stewart Baker: [00:11:20] So, Nick, DHS actually – and it doesn't often happen the government's ahead of the curve, but DHS asked for legislation and got it that allowed it to intercept drones and try to take them down if they intrude into airspace that was critical. I guess my question is: Can they actually do that now that they have the authority?

Maury Shenk: [00:11:43] They can't do it *yet*. The problem is there's two things. You can at least do jamming. So things like what was at the Gatwick Airport, you could actually probably take out with existing tools. You just jam the signal, confuse it, it drops from the sky. The problem is the next generation of attackers respond to jamming with "kill all humans" mode. And so we can no longer rely on jamming. The authorities that DHS got though are wonderfully specific and yet wonderfully broad. It's very specific in where the authority to take down a drone can be used – has to be declared by the secretary and a whole bunch of other hoops to go through. But it's very open in what you can do to take it out. So you can jam it. You could hack it. You could blow it out of the sky. It's designed as a blanket set of authorities that are specific in location in advance – and that location's not delegated downward – but does not presuppose anything on the technology. And there are a lot of people working on better technology

to deal with the problem. And it's really nice to have a legal framework that will allow the government to use whatever technology people like me come up with.

Stewart Baker: [00:13:06] So the thing I was interested in is how hard it was to figure out where the people were. They never did. They thought they had somebody, arrested them, and then let them go. They couldn't figure out who was doing this, who was controlling it, and where. And one of the things that the DHS legislation authorizes is intercepts of the signals between the controller and the drone. And you would have thought that the republic was going to fall if you'd been subscribing to the ACLU and EPIC [Electronic Privacy Information Center] and EFF's [Electronic Frontier Foundation] feeds because they said, "Oh, my God! We can't have that. That's allowing a new wiretap authority." But I think this episode shows exactly why you need that kind of thing.

Nick Weaver: [00:13:48] Yes. And that's the thing. The EFF and other arguments for it neglected the importance of the geographic specificity. It was not a blanket prohibition on enforcement of the Wiretap Act. It was not a blanket cutout. It was very targeted in location, just not targeted in method. And I'm glad that the EFF lost this one.

Stewart Baker: [00:14:15] Well, let me just slide to a different question, Matthew. The Fourth Circuit issued a ruling kind of following on the notion that the president couldn't block people on Twitter, essentially saying the same thing about a county councilman who had maintained a Facebook page for her chairmanship. This is becoming a thing. Is this good law, or are these outlier decisions?

Matthew Heiman: [00:14:46] Well, I mean the Fourth Circuit is certainly in line with the Second Circuit. And so the Second Circuit is where the Trump case is happening. I think the courts recognize that they're sort of aligning around this idea that Facebook or Twitter are public forums for public officials, but also in this Fourth Circuit opinion there was a clear request from the Second Circuit said, "We need help from the Supreme Court," and the Fourth Circuit invited that too. So I think they're all saying, "This is what

we agree on. The courts are aligned, but we're really not sure. And Supreme Court tell us if we're right."

Stewart Baker: [00:15:19] Yeah, I was reading that decision, and I kept thinking to myself, "They're making a big deal about how this is a government-owned forum or a government-controlled forum. And you could solve this problem if you really didn't like the constraints the court put on you just by having people from your campaign paid to maintain the page, and you just say, 'This is the Facebook page of successful candidate for county chair,' and say it's part of my campaign structure, not part of the government. It means you have to pay for it instead of getting the government to pay for it, and maybe they'll make the trade. Maybe they won't." But it's a very funny line that's being drawn. Essentially what this court seems to say is when the county chair sets up a page using her own name and providing the information, if she's doing it as a county chair, that's a government function or a government-controlled forum, and if she did it as an individual, it wouldn't be.

Matthew Heiman: [00:16:25] I think that's right. And I think that's why if I were advising politicians who wanted to have social media platforms, at least until this case shakes out, I think some of the things you mentioned, Stewart, would be helpful to create some daylight. In other words, don't put a lot of stuff in your official capacity as that official. But if you want to use these platforms as a candidate running for office and you want to have your staff maintain it, not you, then that's the way to go. But the reality here is, at least up to now, the courts are saying just because constituents or other users of Facebook and Twitter don't like what you're doing and sending nasty messages, it doesn't allow you to block them. You know I think the other piece of this is – are politicians that thin skinned that they can't deal with a couple of nasty messages on Facebook? I mean I'm not saying that's what the law should be, but it strikes me that you know life would go on if they just ignored those messages. There's certainly no mandate that they engage with these people.

Stewart Baker: [00:17:23] Yeah. So the courts are basically saying, "We don't want public officials censoring their Twitter feed, their Facebook feed, because that's

Facebook job, that's Twitter's job. They'll decide what readers of those social media can say, not to the people they initially said, 'We're going to control it.'" So yeah. Alright. I gotta ask, Nick: The Hal Martin thing, just when you thought it couldn't get any weirder, did.

Nick Weaver: [00:17:50] Yeah.

Stewart Baker: [00:17:52] What happened?

Nick Weaver: [00:17:54] So what happened is apparently the trigger for the initial search warrant was some Twitter DMs [direct messages] between Hal Martin's account and various Kaspersky researchers that were really weird in the sense that it would be like a couple of mysterious DMs and then the Martin account would block the Kaspersky account so that the Kaspersky account could not reply.

Stewart Baker: [00:18:19] Yeah. He wanted to talk to Yevgeny, which is Yevgeny [Eugene] Kaspersky, so it sounded like a high-level reach out. He had some weird stuff in there in which he said you know this offer expires in three weeks. And it came out like a couple of hours before some of the Shadow Brokers leaks. Right?

Nick Weaver: [00:18:40] Yeah. And what apparently happened is Kaspersky told some of their friends in the IC [Intelligence Community], and that's what triggered the eventual search warrant of Martin's house. But it's doubly strange. First of all, that behavior is unusual. Marcy Wheeler has the excellent observation that it could have been somebody compromising the account because, let's face it, the Shadow Brokers have been trolling the NSA for a long time.

Stewart Baker: [00:19:06] But would they troll them by sending messages to Kaspersky?

Nick Weaver: [00:19:11] Maybe? Who knows?

Stewart Baker: [00:19:13] Okay. So there's an elaborate conspiracy theory here that says: The GRU [Russian military intelligence] knew they were going to release Shadow Brokers. They wanted to put the blame on Martin. And they also hoped to make Kaspersky into a hero so nobody would stop using them in the West. And so they took over Hal Martin's account. They sent these fake messages, and then Kaspersky got to play the hero. Is that the conspiracy theory version?

Nick Weaver: [00:19:45] That is the tinfoil hat version. But even the normal version is weird, especially because I'm pretty certain Hal Martin was not the primary source for Shadow Brokers. If you look at the Shadow Brokers' data, it's not normal data pack rat stuff. Three of the four distinct dumps are personalized. Two of them are operator stations where you log into a remote system and set it up as a staging ground. And there's all these notes files, etc., that says what individual was responsible for this data.

Stewart Baker: [00:20:20] And it wasn't Hal Martin.

Nick Weaver: [00:20:21] No. And the SWIFT data was – we know who the guy is. It's some NSA guy, who was in Texas at the time, because his name is over the metadata in the Word document. And this was his system low-side workstation where he was working on a PowerPoint. And we still don't have a good explanation in public for how this data got out at all.

Stewart Baker: [00:20:45] Yeah. So they asked me for comment on the story. And I said what's discouraging about it is that we thought NSA's counterintelligence had gotten really good and they were finding the people who were the sources of all these leaks and that that they got Hal Martin because of their improved capability, and now it turns out they got Hal Martin because he's an idiot.

Nick Weaver: [00:21:07] And in fact, the other thing on Hal Martin is he should have been nailed right at the start. If anything, post-Snowden should have been the ability to detect and mitigate the data pack rats, that when you see somebody accessing too much stuff onto removable media, you just give him a talking to.

Stewart Baker: [00:21:28] Speaking of talking to, Maury, Vietnam says it's going to be talking to Facebook, and fines are in the offing for failing to localize data and to respond immediately to their takedown notices. I know you actually looked at this for a client. How serious is the Vietnamese law?

Maury Shenk: [00:21:49] Well, it's one of these countries, like Turkey is another example that jumps to mind, where they suddenly have a very restrictive regime for content online. It had attracted most attention because of data retention, because it's adopted very broad requirements on communications data that need to be retained and it has to be stored in Vietnam. And a lot of the big US tech companies have admitted that they are out of compliance with that. It also makes illegal a lot of different kinds of content, including anti-government content. And so Facebook, some of its users not unpredictably posted anti-government content in Vietnam. They were notified of it, presumably by the government, didn't take it down fast enough to make the government happy, and you know now they're going after Facebook, presumably with fines. Vietnam is not a colossal market, but it's a pretty big, fast-growing country. And I think it's a pretty big deal for doing Internet business in Vietnam.

Stewart Baker: [00:22:54] Yeah. And they're obviously learning from watching everybody from the EU to the Chinese impose fines on big Internet companies and get what they want, and they figure they're big enough to do that too.

Maury Shenk: [00:23:09] Yeah, I mean anybody who wants to play in these markets, we've seen with Apple recently how subtle changes in a market can have a pretty big effect on commercial results. And so even in a market like that, I think the Internet companies have to pay some attention to those kind of tactics.

Stewart Baker: [00:23:29] So let me ask you about a different regulatory regime. There was a story in Motherboard about how easy it was to get phone location data – maybe not to the level of a Google Maps pinpoint but something that takes you within a few hundred yards – just by buying it very indirectly through services provided by mobile

phone companies. And all of the mobile phone companies have now said, "Oh, yeah, yeah. That thing? We're not doing that anymore." What do you make of that episode?

Maury Shenk: [00:24:04] Well, I've seen this in the UK a number of years ago. This information has been available for a long time. It's base station data, and it triangulates between the various base stations which a mobile is communicating with and takes information from the signal strength and can get a pretty close location – not as good as GPS, but in urban areas it can be down to the tens of meters, and then you send in somebody with a Stingray to find the device if you're law enforcement, a little bit further in rural areas. I was a director of a UK company that used this kind of information for law enforcement purposes, and we complied with UK law. But we bought it through commercial channels. And in the EU, using this for tracking individuals generally requires consent under GDPR. In the US, it's not clear if you can buy the data that you violate any law by figuring out where somebody is located, although the use of the data seems to be grey in terms of the contractual arrangements under which the carriers are distributing it. So this stuff has been out there for a long time, and I think some users might be concerned about it.

Stewart Baker: [00:25:12] So [Senator] Ron Wyden played a big role in trying to get everybody to back down, and I have to say this strikes me as another of his hobby horses where we are going to end up regretting it because there are a lot of valuable things. If somebody is trying to persuade Verizon to switch my phone number to them so they can steal all of my accounts by sending password change requests based on my mobile phone, one of the things that they can do is to check my location. Same thing with banks. If the bank wants to make sure this is the person that they want to be dealing with and that this isn't a fraud, they check to see where the person is located when they're using their phone. At least the third-party uses are going to fail if all of these companies are browbeaten into not providing location data to anybody.

Nick Weaver: [00:26:03] But at the same time, a company can get location data with the user's consent in other ways. So if ever you have an app interface, the app can give location with user consent. The thing is this is non-consensual and being sold to

companies who sell it to sell it to sell it, and it basically is like oil. It's spilled into the ecology, and it spreads everywhere.

Stewart Baker: [00:26:31] That's for sure. Once it's out, it's out. That's what we've learned about data, that you can't really control data. As it gets cheaper, it gets easier. People just start throwing it around. On the other hand, I'm not sure that – let's say you're a bail bondsman looking for somebody who has jumped bail, it's going be a little hard to get consent from them to find their location.

Maury Shenk: [00:26:56] Well, even in the EU, for some of these uses where there are security implications, you can make a pretty strong argument that GDPR permits doing it without consent. I think the issue is, as you and Nick just had an exchange, once it's out there, it's hard to draw the line between the legitimate uses and the problematic uses, and we have to figure out whether there is any way to control that.

Stewart Baker: [00:27:20] Okay. Last: Comic relief: The El Chapo trial is like a guide to weird security problems that you have when you're a narco lord with two mistresses and a wife whom you want to keep track of and an entire secure communication system to set up. And El Chapo seems to have chosen exactly the wrong way to do that. Nick, what did he do?

Nick Weaver: [00:27:48] Well, what he did is he did the thing that the security people say never to do in secure communications, and that was try to do something custom. So he had a dedicated system administrator, dedicated phones, dedicated cryptography of some sort or the other, and this was all fine and good until the Feds flipped El Chapo's sysadmin. And El Chapo's sysadmin happily gave the Feds access to the communications server that acted as the intermediary and could therefore see all of the data because it wasn't actually end-to-end encrypted. So the net result is all the secure communication meant is that it specifically was a secure channel to FBI headquarters.

Stewart Baker: [00:28:35] Matthew, did you ever flip a witness while you were at NSD [National Security Division]? Did you ever take somebody like El Chapo's IT director and say, "We have a deal for you"? Or was that not part of your job description?

Matthew Heiman: [00:28:48] I don't remember ever being involved in something quite like this. It was much more pedestrian.

Stewart Baker: [00:28:54] Yeah. It seems to me for this IT guy to do this to one of the most bloodthirsty narco terrorists around, it must have been a little daunting, unless he just thought, "Well, this guy is too stupid to ever figure out what I'm doing."

Matthew Heiman: [00:29:15] Perhaps. Or he figured, "I'm a dead man either way," because maybe El Chapo wasn't happy with his IT service.

Stewart Baker: [00:29:22] Well, at one point he did say, "You know, Boss, we need to move from Canada to the Netherlands because we'll get better servers there."

Matthew Heiman: [00:29:29] Yep. Well, the other part of story that I just love, Stewart, is the fact that El Chapo had him put a microphone eavesdropping feature on 50 phones so that if you had a conversation with El Chapo, whether you were his girlfriend or one of the deputies pushing drugs, when you hung up and maybe after the boss or boyfriend chewed you out, you said, "Boy, that guy's a real jerk," El Chapo knew.

Stewart Baker: [00:29:52] Because he was listening still!

Matthew Heiman: [00:29:52] Yeah. If you're working for an insecure boss that has you know cartel-like tendencies, just think about that after you hang up. You may still be effectively on the line with your boss.

Nick Weaver: [00:30:04] Especially if your boss gave you the phone.

Stewart Baker: [00:30:06] Exactly. Yeah, that's the problem. On the other hand, you know look, everybody who works for government, their boss gave them the phone, and you know there's a notoriously insecure guy at the top of the government. So you never know. I think those White House secure phones may look more like El Chapo's than you think. I think we ought to cut this off. There are some other great stories. Reid Hoffman is under investigation for basically trying to do what the Russians did, but in 2018 instead of 2016. Huawei's employee has been arrested for espionage in Poland, and Huawei has said he brought disrepute on the company and they fired him. China has [200] million resumes just sitting on a database that nobody understands. No one knows where the database came from or at least who was maintaining it. So the data, it's like an OPM file. It's just sitting there for anybody who wants it. And actually, I'll ask this one question: The Great Firewall is a really interesting story that is going to be a book shortly about how the Great Firewall was weaponized to do DDoS attacks. And I was all over that two or three years ago when that happened, and I was surprised how little response it got in Silicon Valley. It was as though, oh, yes, stuff happens. And, Nick, what's your take on how the Chinese weaponized their Great Firewall? Essentially they said, "If you come to a site from outside China to a site that's inside China, we can inject JavaScript into what you take back, and that will allow us to DDoS people basically using your browser to attack other people in the West in a very distributed way." And I thought that was kind of a creepy misuse of the Great Firewall. Have we seen it since? And should I be worried, or was Silicon Valley right to just shrug it off?

Nick Weaver: [00:32:19] We haven't seen it since, but you should be even more worried because in many ways what the Chinese did was I think the Internet equivalent of Joe-1: Let's set off a nuke but use it to swat some flies. Because the same mechanism that they use could just as easily be used to "oh, this is a visitor from the US State Department. Let's have the JavaScript exploit a vulnerability in their browser and take that over" or "this is an email to somebody in the State Department. Let's modify the Word document that was attached to include malicious code." So there's all sorts of attacks that could have been done with this mechanism that we don't know if they've been done since. But of course, the problem is let's say that we actually do detect this happening, which is hard, what happens is, okay, we complain to the Chinese about this

and the Chinese just respond to the poor State Department official with some Snowden slides because this is stuff that we've been doing too.

Stewart Baker: [00:33:32] So here's my question: Google knows when I go to a site that's on the other side of the Firewall because they know where those sites are. Why doesn't it warn me? Why doesn't it say, "You know we're not going to send you there until you say you're taking the risk that the JavaScript injects are a real possibility and that you may end up as a tool in a Chinese government attack on the *New York Times*," which is what they did last time. Why isn't Google treating this as a health of the 'net problem?

Nick Weaver: [00:34:02] Google is, just in a different way. Chrome now really nags if you're going to a non-encrypted site, and encryption thwarts these attacks. The other problem is just simply avoiding China is not enough because the basic mechanism that it appears the Chinese used, I could basically implement on any modern router that I compromised. I think they took advantage of OpenFlow, which would allow me as a bad guy to get root on a core backbone router and implement the Great Cannon mechanism there. So simply avoiding China doesn't avoid potential attackers. What you need to do is encrypt *all* the data *all* the time *always*.

Stewart Baker: [00:34:53] Okay. And this message brought to you by Signal. Thanks, Nick, thanks, Maury, thanks, Matthew, for joining us. This has been Episode 246 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Please send us suggestions for guest interviews, and we'll send you a Cyberlaw Podcast mug. Send them to CyberlawPodcast@Steptoe.com. Follow me on Twitter [@stewartbaker]. I'm getting better about sending out the stories I think we're going to cover, and you can comment on them. Like them if you think we really should cover them. Give us a rating – we're getting more ratings, and I'm pleased about that – on iTunes, Google Play, Spotify. Leave us reviews. We're glad to get the five stars, but entertaining comments are always welcome, and I will read them on the air, especially if they're entertainingly abusive. Coming up: We're gonna get Jeff Jonas, founder and CEO of Senzing on to talk about disambiguation of identity data; John Carlin – I was hoping to get him on this

week and we may yet – author of *Dawn of the Code War* and former boss of Matthew Heiman, among other things. And finally, our show credits: Laurie Paul and Christie Jorge are the 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.