Steptoe

Episode 223 with David Sanger: A war reporter for the cyber age

Stewart Baker: [00:00:03] Welcome to Episode 223 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking technology, security, privacy, and government. Today I'm joined by our guest interviewee David Sanger, the national security correspondent for *The New York Times* and author of *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. We'll be interviewing him separately after we finish the News Roundup. And then for the News Roundup we have a great team. Pat Derdenger is a partner in our tax practice based in Phoenix who has followed state tax law for his career and who will be explaining the *Wayfair* decision. Michael Vatis, formerly with the FBI and the Justice Department, now a partner in our New York office, who has followed law enforcement access to location data for most of his career and will be explaining the *Carpenter* case. Matthew Heiman, who's a visiting scholar at the National Security Institute at the George Mason University Antonin Scalia Law School, previously a lawyer with the National Security Division at the Department of Justice. Matthew, welcome.

Matthew Heiman: [00:01:15] Thank you.

Stewart Baker: [00:01:16] And Jim Lewis, who is the cybersecurity expert — really for the last 20 years the go-to expert in Washington on cybersecurity issues — operating out of the Center for Strategic and International Studies here in Washington. And I'm your host Stewart Baker, formerly with NSA and DHS and holding the record for returning to Steptoe to practice law more times than any other lawyer. This is Supreme Court week. They're finally getting around to releasing because they have a deadline. All of the hard decisions — all the 5 to 4 decisions — we're going to talk about two of them. This morning I heard that they have, the Supreme Court, 5 to 4 upheld President

Trump's bans on travel into the United States. Not a particularly cyber-ish issue, but if there are a cyber issue elements to it, we'll cover them next week. This week we're going to talk about *Carpenter* and *Wayfair*. Michael, what did *Carpenter* decide, and is it a big deal?

Michael Vatis: [00:02:28] I think it's a very big deal that the Court decided 5 to 4 in a decision — or opinion — authored by Chief Justice Roberts that the government needs a search warrant to get seven days or more of cell site location data from a cell provider. It left open a whole bunch of other questions, but essentially the Court said that despite the fact that cellphone users voluntarily — or despite the fact that cellphone users can be said to provide this cell site location data to the cell providers, they still have a reasonable expectation of privacy in their location information that is basically contained in that data, and so the government needs to get a warrant. But it left open a whole host of questions such as: Does the government need a warrant to get real-time location information from cellphone providers? Does it need a warrant to get less than seven days of historical cell site location information? Does it need a warrant to get other forms of information such as credit card information or bank records that go beyond the fairly limited set of bank records that were at issue in *Miller*? So I think there are a whole lot of questions that are going to be percolating up through the courts now in the aftermath of *Carpenter*.

Stewart Baker: [00:03:55] Yeah, and Justice Roberts probably kept this decision so that he could — this opinion — so that he could write that long paragraph that said, “Now we're only deciding this narrow single question. It doesn't really tell you that third party doctrine is dead. All we're telling you is seven days, that's too much.” It feels to me — and I'm going to say this about *Wayfair* too — that basically the Court has started granting cert and writing opinions that open Pandora's box while they pretend that they've just done something narrow. They're going to leave all of these problems for future Courts and the lower courts to try to figure out, and this one in particular. Everybody was clear on what the third party doctrine was. If you trusted somebody else with your secrets, the government could subpoena them, by and large, unless there was a statute that changed that rule. Now the Court is going to go in and say, "Well, how do

we feel about this kind of secret being trusted to these kind of people and obtained with a subpoena?" They've got 50 cases ahead of them to try to explain what *Carpenter* really means.

Michael Vatis: [00:05:10] Well yeah, I mean I don't think they were faking it when they said the decision was narrow because it is narrowly confined to cell site location data of more than seven days' worth of back activity. But the problem is it leaves so many unanswered questions that the Courts are going to have to wrestle with the implications, and I don't think it's going to be you know Courts' way in the future. I think starting today you're going to see if the government tries to get real-time location data with a 2703-D order or a subpoena or they try to get credit card records with a subpoena, I think you're going to get challenges. If that evidence is turned over by the provider, you're going to get challenges from criminal defendants saying, "Wait a second. I've got a reasonable expectation of privacy because a vast amount of private information that's embedded in those records." I mean think about credit card information. I don't know why location information would be sacrosanct. Your credit card — you know it contains records of everything that we purchase. People increasingly don't use cash. I mean you have your whole life, not just where you go, but everything you buy, everything you do. You don't want a credit card these days.

Stewart Baker: [00:06:33] Well, so here's the problem. For more-or-less 30 years the basic rule has been you gave the record to somebody else, you gave the information to somebody else. The government can subpoena it, and then Congress came along and pretty frequently said, "Well, we think there ought to be some limits on that. We're going to write some rules that say maybe not a warrant but something more than a subpoena. Certain kinds of information is going to be accessible with a subpoena or a national security letter." And they wrote elaborate rules, and they could make perfectly arbitrary rules like six months and suddenly it's available under a subpoena whereas before it required a warrant, etc. And all of those rules you know as a way of responding to new technology that was a pretty smart mechanism. Now we're going to have these 70-year old an 80-year old justices say, "Well, I don't like this technology. This sucks! This is really shocking," and imposing these requirements. And what's more, all of the carefully

constructed congressional compromises that were reached on this are now in doubt because the Court has pulled out the big gun which is it's constitutionally required which means that everything that's in the statutes that we've been relying on for 30 years like the Bank Secrecy Act completely up for grabs.

Michael Vatis: [00:07:58] Well, you know I don't think your complaint really lies with 80-year old justices. I think it really lies with the dead person named James Madison because he wrote the Fourth Amendment, which is all about what's reasonable, what sort of searches are reasonable. And that is a rather expansive concept. And you know it leaves it to courts over the course of history to determine what constitutes a reasonable search, what constitutes a reasonable expectation of privacy, and that that is necessarily going to be elastic and is going to evolve. Even Justice Alito recognizes that. Even the Chief recognizes that.

Stewart Baker: [00:08:35] Let me cite another Founding Father on the question of reasonable expectation of privacy. It was Ben Franklin who said, "Three can keep a secret if two of them are dead." We all learned that in the third grade. If you give somebody your secrets, you are giving them the ability to expose your secrets. That was good enough for Ben Franklin, good enough for me, and I think it was probably good enough for James Madison. Alright. *Wayfair*. Let's move to a slightly less contentious issue but also one where the Court more or less punted. Pat, what did they say?

Pat Derdenger: [00:09:14] Well what the Court in *Wayfair* essentially what they did was to kick out the physical presence test which has been around for some 51 years and said that an economic nexus test suffices for Commerce Clause purposes. Now those of you who buy on the Internet like all of us do, you may have wondered why do some Internet retailers charge a sales tax and others don't. Well it goes back to the *National Bellas Hess* case and the *Quill* case, both US Supreme Court cases in which the Supreme Court laid out the Commerce Clause standard for remote vendors. The first cases, *National Bellas Hess* and *Quill* both dealt with mail order houses, but the Commerce Clause implications of those cases then applied quite nicely you know over

the recent years to Internet retailers. Well, the Supreme Court said that to not unduly burden interstate commerce, a state can impose a sales tax collection obligation on a[n] out-of-state remote retailer only if that remote retailer has physical presence in that state. Well, what the Supremes did in the *Wayfair* case was to negate the physical presence test, said it was wrongly decided to begin with. "We're kicking it out. It's no longer good law, and we are upholding a South Dakota piece of legislation that established what's called an economic nexus test." Economic nexus does not cover physical presence at all. What economic nexus does is essentially says, "Okay, if you're doing business in our state, we're going to be able to tax you." The *Wayfair* Court held that nexus is established when the taxpayer avails itself of a substantial privilege of carrying on business in that jurisdiction. Quite a broad standard now. The South Dakota legislation would have said, "Okay, if you're making sales into our state totaling more than $100,000 for the last year or if you're making individual sales into our state of at least $200 last year, then you're going to be required to collect the South Dakota sales tax on those sales going forward."

Stewart Baker: [00:11:39] So you know I was around for — well at least I remember *Bellas Hess*, and it was reconsidered 25 years later, and the Court said, "You know it might be wrong in *Quill*, but it's been around for 25 years, and we're going to make it so Congress can fix it anytime it wants. And why don't we just leave this to Congress so they can figure out how to decide when it's fair to impose this collection obligation on merchants who may do a small amount of business in a wide variety of states?" And for 25 years Congress did nothing. Now basically the Court is saying it was wrong then, and “We've lost patience. We're going to say it's wrong, overrule it, and we're not going to resolve any of these questions about whether it ought to be $100,000 or $150,000, what are you going to do about local taxes which could be varied” — you could have 100 different local taxes inside South Dakota that people are obligated to collect. So it's really kind of messy for small businesses that haven't been collecting this, isn't it?

Pat Derdenger: [00:12:51] Absolutely. And the Supreme Court in *Wayfair* essentially said, "Okay, we're going to leave those other questions to a future date and a future case. We're not deciding them today."

Stewart Baker: [00:12:59] We're writing the check, and somebody else will cash it.

Pat Derdenger: [00:13:04] Yeah. And you know the check that I personally would hope would be cashed one of these days and fairly soon would be by Congress. As you indicated you know for the last 25 years Congress has done nothing. Will this now be the impetus for Congress finally to do something? I would hope so because under the economic nexus test you know we're in new territory. We're on a new map. We don't know what states are going to do. Are states going to get very aggressive? What if the state says, "Okay, you know if you make one sale into the state that's enough, or you make $10 you know that's sufficient." We don't know the answer to those questions as of yet.

Stewart Baker: [00:13:46] Oh I think I know the answer to that. New York, Illinois, California. Those guys are broke. They're going to ask for every nickel that they can squeeze out of taxpayers is my guess. And you know I actually wrote about the *Quill* decision because I was early to the electronic commerce issue that was decided in '92. And in '94 the Republicans took over Congress, and I said, "You know the idea that a Republican Congress is going to make it easier to collect taxes that they have no role in spending strikes me as extraordinarily unlikely." And for 25 years I was right. Maybe they'll change their mind, but I'm not sure Congress is going to ride to the rescue here.

Pat Derdenger: [00:14:34] Well, I'm not going to hold my breath. I hope they do because under an economic nexus standard we're going to have — economic nexus standards are going to be different from state to state to state. It's going to be a checkerboard. And businesses? They want to comply essentially. And they ask me, "Pat, you know how do I comply? I'm a startup mail order Internet business. You know I'm going to be selling probably into 10 or 20 or 30 states to begin with and hopefully all of them you know in a couple of years. You know how do I comply?" Well, you know the test was physical presence. Let's take a look. Where do you have physical presence? In those states you are going to have to comply. But now you're going to have to take a look at the checkerboard and say, "Okay, do you have $50,000 here? Because that's

the standard in one state. You know $100,000 is the standard in another state." And Congress I hope — and again I'm not holding my breath — I hope they will act to put down a uniform standard for sales tax collection that has to be followed by all 45 states that impose a sales tax. Now Stewart, one thing that I think is very significant from the *Wayfair* case is what the Supreme Court did not do in *Wayfair*. Well, they said that nexus is established when a taxpayer avails itself of the substantial privilege of doing business in a destination state. It never laid out a Commerce Clause minimum standard that needs to be met under the economic nexus test. They left that you know for the future.

Stewart Baker: [00:16:03] Oh it's going to be a festival of litigation over state taxation. Pat, you might want to spell your name for the listeners — that's D-E-R-D-E-N-G-E-R — because you're going to be the busiest man at Steptoe & Johnson.

Pat Derdenger: [00:16:23] Well I can't retire for a long time, can I, Stewart?

Stewart Baker: [00:16:25] No, you're stuck! You're stuck! Okay, speaking of people who aren't showing any signs of retiring. The North Koreans are hacking banks in Latin America and apparently launched massive cyberattacks, probably cyberespionage attacks, in Singapore during the Trump-Kim summit. Matt, Jim: any thoughts about the significance of this? Does this mean that there are limits to the thaw that we're experiencing with North Korea?

Matthew Heiman: [00:17:00] Yes. Next question?

Stewart Baker: [00:17:02] That's good!

Matthew Heiman: [00:17:03] No, I think you know a fish's gotta swim and a dog's gotta bark and North Korea's gotta hack, and I think that's why Singapore had 4.5 times the number of hacks as the US and Canada during that same week. And I think it's a useful reminder for the Trump administration as they try and reach some sort of accord with North Korea on nuclear topics. I hope they don't follow the path of the Obama

administration in terms of what they did with Iran were they focused only on nuclear issues because obviously the cyber issues are not going to go away, and I hope they're thinking about all the issues we have with North Korea, not just in particular the nuclear one.

Stewart Baker: [00:17:39] Jim?

Jim Lewis: [00:17:41] Do you really...? It's bad for the North Koreans to hack into poorly protected banks, but it does serve kind of a useful function because it makes these banks kind of wake up and pay attention. If you look at their victims, they tend to be lower or lower end of the preparedness spectrum.

Stewart Baker: [00:18:00] So this is the argument from Darwin that you're making.

Jim Lewis: [00:18:04] Yeah it's like... And so maybe if Kim's plans to use the thaw to revive the economy come to fruition, they won't need to hack for money anymore, but that will be a long time in the future.

Stewart Baker: [00:18:16] So we are going to interview David Sanger about his new book, and in that book he says the North Koreans (1) should probably get the most improved player award in cyberwarfare. But he also says you know they've — since they don't have an Internet to speak of inside North Korea — they've moved their hackers outside to places like India and Malaysia and Kenya and Poland, for God's sake. I mean I can't help thinking that if that's where they're doing their hacking, we ought to be able to do more than just stop them from breaking into systems. We oughtta be able to bust them. What's preventing that?

Jim Lewis: [00:18:58] Part of it is they don't rely on those places. They kinda map their hacking onto their previously existing black market activities. So where before they did gunrunning or drug smuggling or counterfeiting, they just moved hackers there. But they do have Internet connections in North Korea, and it's a fair question to say, "If we know they're in Poland or if we know they're in one of these places, why don't we lean on the

local authorities to squeeze them?" And you know China — I understand the Chinese would prefer to pretend that the North Koreans aren't there. In places like Malta, they don't want to lose their reputation as a haven for crime. In other places, we might be able to squeeze them a little bit.

Stewart Baker: [00:19:46] I would think so. Poland, for God's sake! That's a Cold War ally that still thinks there's a Cold War on! Alright. So Lightning Round. Lots of quick stories. The Trump administration is considering massive new curbs on Chinese investment, export control rules, on top of all the tariff increases that it has planned. We'll probably get to see more on that. We're just getting bits and pieces, emerging rumors, about what's coming. The administration has said they're going to allow comment from US industry on all of these rules, so that's more or less something we can put on the shelf unless, Jim, you've got something to say about that one.

Jim Lewis: [00:20:39] No, it's just puzzling that with the bill in the Senate moving along — the CFIUS reform bill — that the administration feels the need to do this. Some people have speculated that it might be because if it's an administrative action, they have greater control over it and can use it as a chip. That implies a degree of foresight we haven't seen before, but you know overall it's a good idea to confront China. We'll have to see what the actual proposals look like before we can say whether they'll work or not.

Michael Vatis: [00:21:11] And surely they have exceptions for Kushner properties and Ivanka Trump fashion lines.

Stewart Baker: [00:21:16] Alright, the Democratic National Committee weighs in on that one. Alright, Joshua Schulte...

Michael Vatis: [00:21:24] Just the facts, man!

Stewart Baker: [00:21:24] Just the facts! I am not going to express a view on that one. The guy who leaked massive amounts of very sensitive CIA hacking tools, Joshua

Schulte — he's now been accused of that after having been arrested on child porn — has apparently released, naturally through WikiLeaks, his notes from jail which are every bit the narcissistic self-absorbed "oh poor me" kind of stuff that you'd expect from somebody who has no idea how much damage he's done. You know his diary starts, "Bang! Bang! Bang! I awoke with a start. It's still dark outside. My phone reads 5:30 AM. I jump up and reach for my apartment door, and I see the door unlock. The door opened, and 10 to 12 people in bulletproof vests and guns burst into my apartment. Oh poor me!" And to show you just how sad his lack of perspective is, in his first paragraph he says, "Somehow I doubt Paul Manafort or any wealthy individual suspected of a crime is treated this way," which of course for those who followed that is completely wrong. That's exactly what happened to Paul Manafort. The guy really... There's every reason to think that he's going to deserve everything he gets, and boy, I hope he gets a lot. Chinese hackers are getting stealthier, Taiwan says. Matt, did you read that story?

Matthew Heiman: [00:22:58] I did, and it only makes sense. And obviously Taiwan is an important chess piece in China's ongoing efforts to create hegemony throughout Southeast Asia. And so the fact that they are getting stealthier makes perfect sense. It's the Chinese improvement model, and I would expect to see stealthier hacking not just affect Taiwan but other targets of China's strategic game board.

Stewart Baker: [00:23:27] Well, Jim, there's some suggestions that the Chinese have resumed stealing commercial or quasi-commercial secrets, but that they are being more selective and more stealthy. So that would be consistent with the Taiwanese experience.

Jim Lewis: [00:23:43] Yeah, we probably didn't — we knew that when we got the agreement on commercial espionage that the Chinese would you know be able to re-target their collection resources. And one of the things that led to the agreement was Xi's general discomfort with kind of the very diffuse and unmanaged Chinese commercial espionage effort. So he's been trying as part of his larger reforms with the PLA to make these guys do their day job, and they've gotten better at it. So I don't think — the nose count is that they're still abiding by the agreement, noting that there's wiggle

room on commercial for commercial purposes. So overall they're better, but they seem to be playing by the rules.

Stewart Baker: [00:24:33] So the Justice Department's indictments are playing the same role for crappy Chinese military hackers that North Korean hackers are playing for crappy bank security across the Third World.

Jim Lewis: [00:24:50] The Chinese still complain about the indictments. I was there two or three weeks ago where they brought up the indictments again. "When are you going to lift them?" I always tell them, "Never!"

Stewart Baker: [00:25:04] Exactly. So we're going to be talking more to David Sanger about this because the theme of his book is that we don't have a cyber strategy for fighting in cyberspace and dealing with cyberattacks. But the Congress has come to that same conclusion and has called for a Project Solarium which is a well-known — well, not to me but to Cold Warriors — Eisenhower era effort to figure out what our nuclear strategy should be. They want one for our cyber strategy, and that's in the NDAA. It's almost certainly going to pass. Jim, thoughts on that?

Jim Lewis: [00:25:53] I love intellectual bankruptcy. And so we've got Moonshots and Manhattan Projects. Now we've got Solarium. I mean we should try and go back to the 19th century for analogies as well, don't you think? It's like Hollywood where they can't come up with a new movie. They have to do a remake of a remake. So Solarium Project? Great idea for the 1950s. It is a different century. Maybe the Congress hasn't realized that.

Stewart Baker: [00:26:22] Yeah, I'm very partial to the air war analogy, which I think is a lot more productive than a nuclear war analogy. But that really only gets back to about 1903, so it's not quite a 19th century example.

Jim Lewis: [00:26:39] Solarium really wasn't about nuclear strategy. It was about how to deal with Russia, how to contain them. So it was a well-defined problem where we

had a lot of experience in thinking about how to do this coming out of the Second World War. The rules are very different for cyber conflict because we don't have that much experience. We don't have that kind of background. So don't expect a result that will be permanent.

Stewart Baker: [00:27:05] Alright. Well here's another question that I think you and Michael Vatis and I at least — and probably Matthew as well — all have had our OPM files stolen by the Chinese, and now the files are starting to show up in the hands of criminals. There were some arrests of people who were using it. No obvious connection to the Chinese government, even though everybody believes it was the Chinese who pulled off the hack. Does this mean that the Chinese have gone into a sort of North Korean mode, saying, "Well, why should we just keep this when we can monetize it?" Or are they trying to cover their tracks by turning it over to criminals so they can say, "That wasn't us. That was some criminal"?

Jim Lewis: [00:27:49] It's way too late for that last one. If they were going to do that, they should've done it within the first month.

Matthew Heiman: [00:27:55] That's why I think it's more of a monetization effort. It's: "We've got this asset, why don't we sweat it?"

Stewart Baker: [00:28:01] Right. "I've got this thing. It's golden."

Michael Vatis: [00:28:04] Are we really sure that that data came from the OPM hack? I haven't seen enough details to conclude that.

Stewart Baker: [00:28:11] Apparently, well, we know that they got it from the OPM files, or at least that's the suggestion that the data was OPM data that was being used for ordinary credit fraud.

Michael Vatis: [00:28:27] But I mean not saying it was or wasn't. I'm just wondering how we know that it came from the OPM hack. If somebody has your Social Security

number or your address or your bank account information, you know that may have been among you know — some of that may have been among the OPM data, but it also resides lots of other places that could have been hacked. So I'm just curious how we know this from you know a couple of press reports.

Stewart Baker: [00:28:54] Yeah. So all I know is what the press is reporting which is that it was data stolen from OPM. Fair enough. TBD is my guess. Also TBD is the future of SPLC — the Southern Poverty Law Center, which you guys have heard me rant about as the most irresponsible group in dealing with anti-discrimination issues and hate speech — is now, after settling one libel action, is getting scrutinized by 60 other people that they smeared for libel actions. Couldn't really happen to a nicer group, but there's not much of a cyberlaw connection there, so I'll leave it at that. Algeria shut down their Internet because students were using it to cheat. Everybody in Algeria basically had to stop operating on the Internet because they had an exam, and they couldn't think of any other way to stop kids from trading information about the exam. I don't know what to say. It's seems like an overreaction.

Matthew Heiman: [00:30:03] Especially when I think there are still blue books available to fill out your exam answers, so maybe we need to go back to handing out blue books.

Stewart Baker: [00:30:10] Alright. And the administration is apparently thinking seriously about coming up with some privacy principles that are meant to be a rival to GDPR, which the administration doesn't like because business doesn't like it and because it's a stupid regulation. We haven't heard much about this, Matt.

Matthew Heiman: [00:30:29] No, it seems very embryonic. And it seems like a number of the industry participants that have been in these administration talks don't really know where it's going. I think the practical problem is in terms of any business that's global in scope or even just trading with European customers, the ship's already sailed because as a business matter you're going to set up your data management scheme to the most restrictive standard that way you automatically comply with any lesser standard. So if

the government — if the US government thinks it's going to change that formula, I think they're trudgin' up a steep hill.

Stewart Baker: [00:31:04] Yeah. And look, the Obama administration had the same idea and the same basic stance, which is: GDPR might be okay, but it's a little too much, and why don't we do something that's more reasonable? And it went nowhere. It was too much for business and wouldn't have solved the international problem. Okay. Alright.

Jim Lewis: [00:31:26] I think if we just say "open" and "free" 40- or 50,000 more times, that will change the Europeans' mind.

Stewart Baker: [00:31:33] Open and free Sesame. Yes, I think that's exactly as likely to be effective as anything else that the US government could do in this area.

Jim Lewis: [00:31:43] Too true.

Stewart Baker: [00:31:44] Alright. Our interview this week is with David Sanger, and we're going to be talking to him about his new book, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. David, your book, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, is in many respects a continuation of your earlier book, *Confront and Conceal*, and it's the history of cyberwar over the last three or four years. What's the theme?

David Sanger: [00:32:15] So, first, thanks for having me back on, Stewart.

Stewart Baker: [00:32:19] You keep writing the books, we'll keep putting you on.

David Sanger: [00:32:21] Well, okay, that seems like a reasonable deal. It takes longer to write the books than to talk about them for some odd reason. Yeah. So the last book, *Confront and Conceal*, was really a history of Obama's foreign policy during his first term, and it happened to be remembered for the revelations about his role in Olympic

Games which of course was the attack on Iran's nuclear program. But at the time that I wrote that book — and it came out six years ago this month — it was hard to find another sophisticated state-on-state cyberattack. There were some denial of service attacks so forth and so on. But nothing you'd sort of step back and say, "Oh, wow. That's impressive."

Stewart Baker: [00:33:07] Right.

David Sanger: [00:33:07] Okay? And now in the six years that have come, there have been hundreds that we just know about. And then of course all the ones that we don't know about. And this has gone from a capability that belonged to the United States, Britain, Israel, Russia, China, to a lesser degree six years ago Iran, and North Korea, to one 30 or 40 states have: the ability to do somewhat sophisticated cyber operations, some more sophisticated than others. And suddenly we have a US government that has built up a significantly powerful US Cyber Command but can't really show you the strategy and the deterrence theory that runs behind it. Similar to the nuclear age, we get our weapons first and our strategy second.

Stewart Baker: [00:34:07] Yeah, but a lot less successfully, looks like.

David Sanger: [00:34:08] Now, remember — and one of the things I went back to read before I sat down to write this book. I went back to read Henry Kissinger's *Nuclear Weapons and Foreign Policy* which was written in 1957, and it was the first real popular book that he had published. He had published his work about Metternich after graduating from Harvard, but I would not call it light reading. It's not good summer beach reading. It's interesting, but it's not summer beach reading. *Nuclear Weapons and Foreign Policy*, which came out 12 years after we dropped the bomb on Hiroshima and Nagasaki, was an effort to say, "Hey, this has fundamentally changed the way we think about national security. This is more than just a new weapon. It's a weapon that changes the capabilities of different states."

Stewart Baker: [00:34:55] And we kind of knew it, but he articulated...

David Sanger: [00:34:57] He articulated it, and then he laid out some theories, some of which I think come to rethink or restate that included some arguments about why we could conduct limited nuclear war, wouldn't probably stand up quite as well today. But nonetheless, it's a pretty remarkable work. And as I was reading, I was thinking to myself, you know where we are in the cyber age right now is we have a lot of people writing about how to protect yourself, how to protect your networks, how to do two factor authentication. You know writing about individual hacks, but no real explanation about what has changed geopolitically that is making this the perfect weapon. The perfect weapon for weak states that want to attack much bigger states. The perfect weapon for states that know they can't afford to get into a direct conflict with the United States but need something that they can dial down or dial up. And I thought, you know the years since *Confront and Conceal*, since Stuxnet gave states the excuse they were looking for to do what they were planning on doing anyway, needed a book.

Stewart Baker: [00:36:06] So the theme as I saw it was: What is this strategy? Look, it's a great book with lots of anecdotes, and it doesn't get hung up on strategy as a grand theory, but that is the thread that runs through it — that we need to figure out how we're going to address this.

David Sanger: [00:36:29] We have enormously powerful weapons in search of a guiding principle about how we're going to use them.

Stewart Baker: [00:36:36] And increasingly when people talk about deterrence, which has always been part of discussions since that is more or less the nuclear strategy, it turns out that the nation that you can point to as having been deterred most in cyberattacks is the United States.

David Sanger: [00:36:59] Right. Because we're the most vulnerable. Our cybersecurity has certainly improved over the past few years, but the target space in the United States has expanded far more quickly than our cybersecurity has improved. So while we're getting better, we're becoming more vulnerable faster than we're getting better.

And that's because we've got Internet-connected cars, and we have Internet-connected security cameras on the outside of our houses that can be turned into basically driving bots. Right? And we have Internet-connected refrigerators. For the life of me I can't figure out why I want an Internet-connected refrigerator, but go online and there are a lot of them for sale.

Stewart Baker: [00:37:46] And you're going to have trouble buying one that isn't.

David Sanger: [00:37:48] That's right. And every one of these comes with a different level of security or no security at all or the password is "refrigerator." And so the difficulty that we're facing now is that if we do something, the ability to escalate is so much greater. And this paralyzed President Obama more than once. So the Russia hack chapters begin — well, they begin in Ukraine in a chapter called "Putin's Petri Dish" because every single thing the Russians did to us...

Stewart Baker: [00:38:26] They tried out first in Ukraine.

David Sanger: [00:38:29] Absolutely. And if you were paying attention in Ukraine, you would have had the complete roadmap to the Russian strategy for the United States. But we did not imagine...

Stewart Baker: [00:38:39] That it would work. We didn't think it would work.

David Sanger: [00:38:40] We didn't think it would work. We didn't even think that they had the nerve to leap the Atlantic and do it here, even if they thought it might work. Then as you go into these chapters, I take you through the hacks that preceded the DNC, White House, State Department, Joint Chiefs of Staff. And what do they all have in common? That the Russians go into them. That the US fights them off. There's fun stories in here about a two-week battle to get them out of the White House system. It's not that getting them out was that hard. They just kept coming back to prove that they could.

Stewart Baker: [00:39:14] Right. And that was really a difference in style between the old Russian intelligence collection mode in which getting caught was the worst thing that could happen, and they realized as they kept fighting to get back in that getting caught had no price at all.

David Sanger: [00:39:31] You know the subtitle, as you said before, was "War, Sabotage, and Fear." This wasn't an act of war. It was on its way to being an act of sabotage. But what it really was about was creating the fear that they could get into any of our systems. And fear is critical here because if you don't have confidence in the systems that run your daily life, then you change your behavior. If you don't believe that when you pull the lever for whatever candidate you're voting for, that you are necessarily going to have your vote counted for that candidate. If you think that when you step into your autonomous car, it might take you to a supermarket where you intend to go, but it may take you off a cliff where you really don't intend to go, then it suddenly undercuts your confidence in all of the basic systems around you. And that's really what the Russians had in mind here. It wasn't to go win some huge victory in which they unplug everything from Boston to Washington.

Stewart Baker: [00:40:33] So the story of the Obama administration's response to the Russian attacks is one of the more dramatic ones. And there's — one of the things that struck me about the Obama administration's approach to this that undercut them further was the extent to which they thought that law would save them, that if they could make things a violation of international law, then they could object to them, and they could stomp their fists and insist that it end. And so they kept looking for things that violate international law, but one of the things that doesn't violate international law is breaking into somebody's system and stealing secrets. And time and again, you have a couple of quotes here, the president, his intelligence officials say about things like the intrusion into the White House system or the DNC or the OPM hacks, "Well it's espionage. We do it too." And then they act as though having said that, there's nothing more they can do about it.

David Sanger: [00:41:45] That's right. And in some of the cases, it started as espionage but didn't end up as espionage. Okay? So Jim Clapper made exactly that argument you know about the OPM hack the Chinese did and basically said if we could have gotten into the system, we would have as well. I would argue that when you are collecting the vast amounts of data, far more than just Social Security numbers and dates of birth and all that, on seven percent of the US population — the elite seven percent that have security clearances — I'm sure your stuff is sitting off in Beijing right now, right?

Stewart Baker: [00:42:21] I'm increasingly afraid it's being used for credit fraud and tax, too.

David Sanger: [00:42:27] That's the interesting thing. Nothing that was stolen from OPM...

Stewart Baker: [00:42:32] ...until this week...

David Sanger: [00:42:32] …has ever shown up until this week, and we actually don't think that that was out of the Chinese part of the hack.

Stewart Baker: [00:42:37] Oh, okay. Somebody else did that.

David Sanger: [00:42:37] We think some — it may have been out of the investigation into them and some of the others. Okay? But almost nothing from the Chinese part of the hack has shown up on the Dark Web for sale. And of course how did the US government respond to losing the data on seven percent of the US population?

Stewart Baker: [00:42:57] Oh, I know. I got caught monitoring for a year.

David Sanger: [00:43:01] You got free credit monitoring for a year. Well, thank you very much for something that actually didn't address the question. And did the US government ever step out and say it was the Chinese? Only once when Jim Clapper

made a mistake and was later forced to back off from it. Okay? But the fact of the matter is that I think that was more than just espionage because at that moment you are building a giant database that you are then applying Big Data properties to, probably combining with what they stole from Anthem and all the other insurers, to get a picture of who worked on what and then begin to use it for all kinds of other purposes. So it's right in that gray area between espionage and active measures. Similarly for the Russia hack, the initial thinking was, "Well, they were going into the White House, the State Department. We don't need to name them because it's just espionage." Well what lesson did Vladimir Putin emerge from that with? "Well, these guys aren't going to name us and penalize us for going into the White House and into the Joint Chiefs of Staff and into the State Department. Who's going to care about the DNC which is basically staffed by a bunch of college kids and constantly broke?" So I think the lesson Putin emerged from was there's no price to pay. Let's go for it.

Stewart Baker: [00:44:19] Yeah, and it turned out there wasn't. Really the right answer is not: is this a violation of international law? That's why you can't do it to us. If I can indulge my inner Trump, maybe not inner — it's because we're the United States of Goddamn America. You don't do that to us because we will make you pay if you do. That's the right answer, and unfortunately we had no way to make them pay or didn't think we did. And that was the other disincentive they could think of a hundred things that Vladimir Putin could do in response to the many things that we could have done to make him pay a price.

David Sanger: [00:44:57] So the deep fear in the White House at the time was that Putin would come back on election day and play into the Trump meme that someone was rigging the election. And since it was clear to everybody in the Obama White House that Hillary Clinton was going to win, why play to that theme when you could punish the Russians after election day and then hand the plan for punishing them further over to Hillary who would then continue it?

Stewart Baker: [00:45:27] We'll give this to the Goldwater Girl and she'll treat Putin the way he deserves.

David Sanger: [00:45:32] That's right. So in the end, it turned out things didn't work that way. And so they rushed to try to come up with some sanctions against Putin that they enacted in the last days of the Obama presidency, and I quote one of Obama's aides in here after they threw out the 35 Russian spies who were allegedly diplomats and closed down two facilities including one in which the Russians were digging underground to get into or underground cables. One of these officials said to me, "It was the perfect 19th century response to a 21st century problem."

Stewart Baker: [00:46:08] Well usually we're within a 100 years of the public response. Yeah, and the response to some of this stuff — the president said, "Well you can't go into intermediate countries' computers to strike at Russia because that might violate international law. We have to get permission from every country that has a computer that might be a good way to get to the Russians."

David Sanger: [00:46:39] So this came up in two distinct cases. One was the failed effort to go after ISIS where a lot of the stuff was stored in places like Germany, and the concern was: do we need to tell Germans we were coming through the system? The president decided, yes you needed to. The other was going after North Korea in response to the Sony hack where you can't get into the North Korean networks unless you go through China because that's where all of the connections come out. And there they got the Chinese to actually cooperate in shutting the North Koreans down for a couple of days. But I mean, big deal.

Stewart Baker: [00:47:15] So that was — yeah, if the Chinese are letting them operate on their territory, they really should not be surprised if we go onto their territory to respond. This is what we said to Pakistan when we were going into Afghanistan.

David Sanger: [00:47:27] I was about to say that that the analogy here is counterterrorism. And I don't remember that US Special Forces asked for a permission slip from the Pakistani military.

Stewart Baker: [00:47:39] So let's talk about China because they are all through this book as well. And the thing that surprised me — there are lots of tidbits in here that I'd never seen before — the stuff that Snowden disclosed about US activities in or relating to China got no press — probably because there was no way to make them a scandal — in the United States. But they got enormous coverage — or at least really shook the Chinese — when they discovered for example that the US government had data centers in China that it was using to serve malware.

David Sanger: [00:48:19] We got into Huawei. I mean all this time, the US government has been warning everybody not to buy Huawei equipment, and the NSA was deep inside Huawei to figure out how Huawei equipment worked and who ran Huawei.

Stewart Baker: [00:48:32] Yeah. Well, the thing that I was astonished by: the Chinese have mobile nuclear missiles that they shuttle around the country in order to keep us from taking them out in a strike. And the people who are shuttling them around all have cellphones. And apparently we were keeping track of their missiles by keeping track of their cellphones.

David Sanger: [00:48:55] You know, it's a little bit like — you remember about a year ago, there was this great — maybe even less than a year ago — the heat map that came out from Fitbase where you could see everybody's Fitbit...

Stewart Baker: [00:49:06] ...all the running tracks...

David Sanger: [00:49:08] ...all the running tracks...

Stewart Baker: [00:49:08] …and all the unacknowledged bases.

David Sanger: [00:49:10] Right, and so we were just trying an experiment with that map, and we found people jogging around the perimeter in Turkey out at the Incirlik Air Base where we keep our unacknowledged nuclear weapons stores in Turkey. Separate broadcast for a separate time: why are we keeping nuclear weapons in Turkey under

current conditions? But we'll set that aside. So this has become a great method for understanding military operations because everybody's carrying their own little electronic, digital dust with them

Stewart Baker: [00:49:45] I mean it does actually — well it doesn't make me rethink Snowden because I have a view of Snowden — but it oughtta make a reasonable person rethink their view of Snowden that he would release that kind of information.

David Sanger: [00:49:58] I don't think he knew. You know the thing about Snowden was he didn't go through most of this data. He sort of handed it out and said, "You journalists make up your mind about what's newsworthy here or not." I don't think that he had the slightest knowledge of 90%...

Stewart Baker: [00:50:14] So when we can find Glenn Greenwald's sense of patriotism?

David Sanger: [00:50:18] And Laura Poitras and many others who had control over it. But the fact of matter is there was a lot in there. Now, I do have to say, the Huawei story? We ran on the front page of *the New York Times*.

Stewart Baker: [00:50:29] I remember that.

David Sanger: [00:50:30] But by and large most media was so focused on — understandably — the privacy aspect of the Snowden thing that what I thought was really revealing about the Snowden trove — which was what it told you about our offensive capabilities — was largely lost.

Stewart Baker: [00:50:47] Because people didn't want to turn him from a hero into a more ambiguous figure.

David Sanger: [00:50:51] He was ambiguous.

Stewart Baker: [00:50:51] He was, for sure. Toward the end of the book, you talk a little bit about China's Silicon Valley strategy and the extent to which the Pentagon is discovering that China's ahead of it in wooing Silicon Valley and gaining access to new technologies, little change in military planning. And you kind of provide the intellectual heritage or origins of all the stuff that we're seeing now with respect to changing the rules on CFIUS and the intellectual property rules. A lot grew out of the Pentagon's discovery under Ash Carter that the Chinese were eating our lunch in Silicon Valley.

David Sanger: [00:51:44] Right. So Ash set up — Ash Carter, Defense Secretary — set up a unit called DIUX — in that wonderful Pentagon-ese, it's Defense Industrial Unit Experimental. And the first thing to know about them was they looked around and they couldn't afford the rent in Silicon Valley.

Stewart Baker: [00:52:02] Of course not!

David Sanger: [00:52:03] Of course not! So they found an old like disused Air National Guard Unit. I think it was a building that's just outside Moffett Air Force Base, wasn't inside the gate. But they could get it — the rent was cheap. And what cracked me up the first time I went to go visit it was that as you drive in — I'm looking up at this building. I've been in this building next door. What is it? It's a Google building. And I realized it was the building where Google had set up its anti-NSA unit after the Snowden disclosures and had the team which is described in the book who were working on sealing up Google's system so the NSA could no longer get in between its servers and so forth. So the distance between that and the DIUX thing was maybe 200 feet, window to window.

Stewart Baker: [00:52:58] So a little laser listening device would really plug back out.

David Sanger: [00:53:01] So they were working on all kinds of interesting technologies. This was a very good initiative to say, "Look, there are a lot of technologies that are already built for commercial purposes that we could just adopt for the military and do cheaply." One of them which Bill Broad and I wrote about was putting up inexpensive

synthetic aperture radar over North Korea so that you could see the missile movements and so forth.

Stewart Baker: [00:53:25] This is with the little mini-sats?

David Sanger: [00:53:28] Mini-sats that are right now used to count cars over you know Sears parking lots to try to figure out how long it's gonna take Sears to go out of a business.

Stewart Baker: [00:53:37] I'm on the advisory board of a company that's doing something like that, and it's dirt cheap.

David Sanger: [00:53:41] It is. And of course the big satellite makers who are selling satellites for $5 billion apiece to the Pentagon are less than enthused about the development of this technology.

Stewart Baker: [00:53:51] But you know they're so predictable. I remember the North Koreans one time when they knew the satellite that was watching them was overhead went out and did a military formation with their troops that spelled out a rude greeting to the Americans.

David Sanger: [00:54:08] You know those North Koreans — we're going to miss them one day.

Stewart Baker: [00:54:11] I would look forward to that!

David Sanger: [00:54:14] But at the end of the Obama administration, DIUX commissioned a study of Chinese activity, and it was initially classified. It's now declassified. You can find it on the DIUX website. And it was remarkable because the Chinese had looked at for example our CFIUS regulations — the Committee for Foreign Investment the United States — and concluded that you really only have to report when you've invested in more than 50% of a company. And they're thinking, "Who wants to

invest in 50% of a company?" So they started up venture capital firms in Silicon Valley with perfectly American sounding names. And sooner or later, all of these companies that needed funding were putting their business proposals right through them, which was 90% of what they needed to go see. And sometimes they took a 10 or 20% stake in the new company, which didn't require CFIUS reporting.

Stewart Baker: [00:55:09] As a technical matter, under CFIUS, if you're over 10%, you run the risk if you don't file. So if you got 40%, CFIUS would always consider control. And now with the Chinese, if you go over 10% they're going to find control. But for sure there was a...

David Sanger: [00:55:28] There was a real sort of below-the-radar operation here. And frankly, we're not in a position where we want to cut off all foreign venture capital coming into the United States whether it's Chinese, European, Japanese, or anything else. But it was just a fascinating, very detailed strategy. They had figured out how to game the system to their great advantage.

Stewart Baker: [00:55:52] So I'll chide you for one passage in your book where...

David Sanger: [00:55:57] Only one?

Stewart Baker: [00:55:58] I've got others, but only one on the air. Because after all this, Senator Cornyn begins work on CFIUS reform, and the Trump administration comes in and gives his effort a giant bear hug. "This is what we want." And does a lot of things in parallel to that. And instead of saying as you've said about DIUX — a very thoughtful, careful, important topic — you say, "This was an excuse for protectionism for the Trump administration." I think you've gotta give the Trump administration credit. Sometimes they're going to find an acorn.

David Sanger: [00:56:40] No, I think that they do deserve some credit, and this had begun in Congress before them. When the Obama administration started this down the road, they realized CFIUS needed to be done. What worries me about the Trump

administration is not actually their CFIUS reform. I actually think that's fine. What worries me is their loss of focus on every other cyber issue that I've put in here. What happened after John Bolton came in as the national security adviser? He got rid of the homeland security adviser who had a significant cyber ambassador, Tom Bossert. That's fine. He gets to choose these, though I think what bothered him about Bossert was that he had direct access to the president. And I haven't run into anybody yet who said Bossert was doing a bad job.

Stewart Baker: [00:57:20] Right. I think we're now hearing the next hints of the next book because none of this is in the book.

David Sanger: [00:57:26] No, no. Actually the Bossert thing is the very end because it happened just as the book was closing. And then he got rid of the man who was the cyber coordinator, Rob Joyce, who had run the TAO, the Tailored Access Operations unit.

Stewart Baker: [00:57:41] So he really knew these issues.

David Sanger: [00:57:42] If you're going to build defenses, the first thing you want to do is hire somebody who has been spending their life doing offense. Right? He went back to the NSA, and then they eliminated that position.

Stewart Baker: [00:57:52] I know.

David Sanger: [00:57:53] And the answer they gave me was, "Well, cyber is part of everything, so we don't really need one." And I said, "Well, you think we're over-coordinated in the US government on cyber right now?" I didn't get an answer to that.

Stewart Baker: [00:58:04] So Cyber Command is another issue that came up in the Obama administration. It was created in the Obama administration. It's continuing into the Trump administration. And you're pretty hard on them, and I'm not going to say unfairly hard. But the impression that comes out of the book is that they're a little

hapless, that they don't have tools that really are highly effective when they launch them, they're more likely to wipe out valuable sources of intelligence than to achieve long-term military effect. What's your overall impression about Cyber Command, and what do we need to do to fix it?

David Sanger: [00:58:45] Well, first of all it's got a very good, very talented person running it now in General Paul Nakasone. You'll read about him in the book and a little bit of his history, and he oversaw Nitro Zeus which was a classified program to basically unplug Iran if Iran got into a big conflict with the US. And they were able to put that on the back shelf after the 2015 nuclear agreement. Now I hear that agreement's run into a few issues, so I don't know if they're dusting it back off. But Nakasone knows what he's doing, and he understands — he ran Army Cyber — he understands the problems that come from Cyber Command's over-dependency on the talent inside the NSA. And they've basically got to decide whether that is a continuing problem or whether they're going to sort of live with it and try to figure out how to integrate these two, even the one's a military and one's largely an intelligence unit. Building a repetitive capability inside Cyber Command that just replicates what's in NSA doesn't sound to me like an effective way to use the taxpayers' money.

Stewart Baker: [00:59:53] Well you've got — if you're going to do espionage, you've got to get in first. If you're going to do an attack, you gotta get in first. So the getting in stuff oughtta be the same.

David Sanger: [01:00:04] Right.

Stewart Baker: [01:00:05] It's what you do when you're in — and in many cases, yes then you'll need — you know if you're going to wipe, if you're gonna brick everybody's machine, then you need a different tool from stealing all the secrets.

David Sanger: [01:00:16] That's right. And you're going to have this constant conflict between whether it's more valuable from a national security perspective to stay inside and watch what your adversary is doing or reveal yourself by shutting them down.

Stewart Baker: [01:00:28] So speaking of that, toward the end of the book, you write about the North Korean missile program that had an 88% percent failure rate. And you almost, but don't quite say, that the US government caused that with a cyberattack. Do you think that the US government had a cyber program that succeeded?

David Sanger: [01:00:56] Yes. So we certainly had a cyber program, and I say in the book outright, President Obama accelerated this program in orders that he issued in January of 2014. And it was aimed at the Musudan missile program, and that's the one that had the 88% failure rate. The problem that they ran into at the Pentagon, the NSA, every place else, was proving that any individual failure in those tests was because of our cyberattacks because it could have been because of bad parts, some of which we were sending in. It could have been because of bad engineering. It could have been because of an insider in North Korea who was undermining things. It could have been because somebody made a plain old mistake. We've blown up plenty of missiles.

Stewart Baker: [01:01:37] Although I think you know the test that proves that we did have a program on that basis is the fact that when he went to a different missile, that we didn't know about apparently, he had an 88% success rate, which is why you know we ended up feeling the need to lean on him and talk to him.

David Sanger: [01:01:56] So I certainly came out of this believing that some of that 88% was because of our cyber program. Could I tell you what percentage it was? I can't, and I'm not sure even the people who do the program can with any certainty give you those numbers.

Stewart Baker: [01:02:11] But, boy, if the North Koreans — who are enormously paranoid and believe in air gaps and anything you could do to keep the US government from affecting their missile program — and the Iranians — who also were into air gaps and did everything they could to keep us from their enrichment program — couldn't keep us out of their systems, their essential national security systems, what does that say about the security of our missile launch systems?

David Sanger: [01:02:43] Well, and what does it say about the precedent we have set by going in to use cyber against command and control and similar systems?

Stewart Baker: [01:02:51] Oh, that is so Obama administrations to say, "Oh, well if we do it, others will do it." If we don't do it, others will do it!

David Sanger: [01:02:56] Others will do it as well. Right. But it does make it hard to create a norm that walls this off. And one thing I hear from people is...

Stewart Baker: [01:03:05] Who's going to be enforcing the norm if our nuclear missiles don't fire?

David Sanger: [01:03:09] It will be a very brief enforcement period. I agree. So this is sort of where the book ends. Everybody loves to talk about setting norms in this area. And then you ask the question: why hasn't this happened? Why don't we have our Geneva Convention already? And the answer to that is: a lot of things we don't want to see foreigners do to us, we don't want to lose the ability to do to them. So if we were to set some norms... Let's say you and I, Stewart, you know went downstairs after — because we would only do this after hours, Stewart — and bought a beer and made a list of things that we thought should be walled off. So we'd say: election systems? Check. Hospitals? Check. Emergency service responders? Check. And I'm sure you and I can come up with a half-dozen more. And then you turn this list over to your old colleagues in the intelligence community and said, "We're going to go out and negotiate this set of norms. You guys got any problem?" I think there'd be a phone call coming back and saying, "Stewart, you know this election system thing? I realize Russians — our election was you know it was ugly. Do we really want to give that up? Because remember we did it in Italy in the '40s, in Latin America in the '50s and '60s, in Iran in the '50s." Hell, we ran a coup in Iran.

Stewart Baker: [01:04:34] Kermit Roosevelt ran it.

David Sanger: [01:04:36] Right. I'm not really grandson of. "I'm not really sure we necessarily want to give this up."

Stewart Baker: [01:04:47] So if we're not going to give it up...

David Sanger: [01:04:49] Right.

Stewart Baker: [01:04:49] ...then we have got to live with the consequence of being attacked. We have to be prepared to accept the consequences of escalation.

David Sanger: [01:04:57] So when was the last politician you heard who said, "My fellow Americans, I realize you're all very unhappy because you realize that your credit cards are getting stolen and you're the collateral damage in this war between states going on 30,000 feet. And I'd love to stop it for you, but frankly I'd rather keep the option open to be able to do this to other countries. So just live with it."

Stewart Baker: [01:05:19] So there's a substantial Jacksonian element in the United States who would be delighted if you said, "Those sons of bitches are stealing your credit cards and interfering with our elections, and we're going to do it to them, only twice as hard and make them pay. And that means we're going to suffer ourselves because those sons of bitches are going to fight back, but we will win. Let's go kick some butt." I don't know if that's a winning argument. But...

David Sanger: [01:05:49] What did Barack Obama used to say? He used to say the problem with the Internet is it's the Wild Wild West. Well, you would make it wilder and wilder. I mean that is the Internet equivalent of "Let's arm teachers."

Stewart Baker: [01:06:02] Yes. But I'm not sure we have the same view of that. Alright. David, this has been a fascinating conversation. There's so much more in the book that we didn't get to talk about. I'm really sorry that we missed it. But if you follow this area, this is required reading to catch up on all the anecdotes you left out of your *New York*

Times articles plus some new reporting. So my thanks — oh, David do you have any events coming up? Are you going to be doing any readings?

David Sanger: [01:06:34] So you know most book tours are done on podcasts like yours or on TV or radio. But on this Thursday evening, the 28th, I'm going to be at Politics and Prose here in Washington, DC, and we should have a lot of fun there. It's a good place for the Washington community to come back and talk, and I'm sure I'll have some more as the school year starts up.

Stewart Baker: [01:06:58] I'm sure nobody at Politics Prose will criticize you for the things I criticized you for.

David Sanger: [01:07:04] I'm sure that we'll find a few.

Stewart Baker: [01:07:08] Alright thanks to David Sanger...

David Sanger: [01:07:10] Thank you.

Stewart Baker: [01:07:11] ...the author of *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Also to Pat Derdenger, to Michael Vatis, to Matthew Heiman for joining me on the News Roundup. Thanks to Jim Lewis who showed up with little advance publicity. He also joined us in the News Roundup. This has been Episode 223 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Send us your suggestions for additional speakers at cyberlawpodcast@steptoe.com. If we get that person on the show, we'll send you a highly coveted Cyberlaw Podcast mug. David of course has an entire serving set of podcast mugs. And if you want to give us a call and hear your voice, your message has got to be entertaining. It can be abusive, but it's gotta be entertainingly abusive. Call us and leave a message on 202-862-5785. Rate the show on Google Play or iTunes so that we'll get more listeners who can find out about us. We've got upcoming guest interviews: Matt Waxman and Duncan Hollis are going to be talking about their latest paper about cyberwar. Mike Hayden is going to talk about his new book about intelligence and the Trump administration. Woody Hartzog of

Northeastern University, who's written a book on privacy by design, is also going to be on. Bobby Chesney and Daniel Citron are going to talk about deep fakes. For those of you who only come to The Cyberlaw Podcast for the sex, that'll be a great one because deep fakes is mostly about putting other famous peoples' faces on porn actors in a persuasive way. We're going to have Noah Phillips, FTC Commissioner. And I think we're doing all that before we go on our August break. We've also got our request back in for rescheduling with Kirstjen Nielsen who is having trouble getting a meal in this town, but we promise we will serve her a meal if she comes. Finally show credits: Laurie Paul and Christie Jorge are the producers; Doug Pickett is our audio engineer; Michael Beaver is our intern; and I'm Stewart Baker, your host. We hope you'll join us in the next episode and all of those upcoming interviews as we once again provide insights into the latest events in technology, security, privacy, and government.