Demetri Kofinas:	00:00:00	Today's episode of Hidden Forces is made possible by listeners like you. For more information about this week's episode or for easy access to related programming, visit our website at hiddenforces.io and subscribe to our free email list. If you listen to the show on your Apple Podcast app, remember, you can give us a review. Each review helps more people find the show and join our amazing community. And with that, please enjoy this week's episode.
Bruce Schneier:	00:00:31	In the summer of 2017, a weapon of war was dropped on to a world without borders, where the heavy artillery and nuclear warheads that defined the battle lines of the 20th century had been rendered useless. The attack, known as NotPetya is estimated to have cost its victims $10 billion in damages, a fraction of the 600 billion that a recent report for the Center for Strategic and International Studies estimates as the annual cause of cybercrime. Nearly 1% of global GDP.
Bruce Schneier:	00:01:10	While the cost are enormous, they are still manageable and more importantly, they pass largely unnoticed. The public, lacking context for each new attack, remains blind to the gathering threat, unable to appreciate the gravity of a cyber 9/11.
Bruce Schneier:	00:01:29	Until now, crime and terrorism on the internet has been measured in dollars and cents, but what happens when we begin to measure it in terms of flesh and blood? The 20th century saw its share of industrial innovation and forward progress, but for the most part, those changes were discrete. Things got bigger, faster, cheaper, and more luxurious, but no one would ever say that a train became a toaster or that a pacemaker turned into an aisle of books.
Bruce Schneier:	00:02:01	The composition of an object, its components parts, did not exist independently of its used case. A key used to open a gym locker couldn't be repurposed to start a minivan nor can a refrigerator open the door to a power plant or the holes of Congress. In today's world where everything is a computer, everything is vulnerable, and when those things are connected to the internet, everyone is exposed. This week, on Hidden Forces: Bruce Schneier, cyberwar security, and survival in a hyper-connected world.
Demetri Kofinas:	00:02:55	Bruce Schneier, welcome to Hidden Forces.
Bruce Schneier:	00:02:57	Thanks for having me.

Demetri Kofinas:	00:02:58	It's great having you on the program.
Bruce Schneier:	00:03:00	Yeah. So far so good.
Demetri Kofinas:	00:03:02	I don't want to jinx it but you're with a new book, and I going to show here for our video viewers. The book is called Click Here to Kill Everybody. This is what? Your 15th book?
Bruce Schneier:	00:03:12	You know what, it's surprisingly hard to count, I'd say about a dozen. Let's leave it at that.
Demetri Kofinas:	00:03:16	I think your publisher told me 15. That's quite a title. I suppose the first question is, why that title? The second question is, why didn't you feel compelled to write a book? I think, three years or less than three years after your last one, which was Data and Goliath.
Bruce Schneier:	00:03:29	The title is admittedly click-bait, right? That's a title that has curb appeal and I'm really speaking to a world of dangerous computers that can fail catastrophically, so I want to evoke that. And I actually do like the cover, I like it for two reasons: one, there's only one button that says okay, when it's not okay and it also looks like this thing's been throwing error messages the best two hours and no one's been reading them.
Bruce Schneier:	00:03:54	So this book is about safety, really. My previous book was about data and privacy, about surveillance. This book is about physically capable computers and safety. So it's a very different topic and a lot has changed in the past few years. Computers now affect the world in a direct physical manner and that brings new risks, and that's what I want to talk about. The new risks and the policy measures we have to think about to mitigate them.
Demetri Kofinas:	00:04:26	It's interesting when you're talking, like there was a quote either in the book when I was the book or somewhere else that I got of yours and I have it right here. It is, "You're right, the internet is no longer that other place that we had the luxury to enter and exit and at our discretion, increasingly it is the world we inhabit." And there's definitely a some something in the book where you talk about going on the internet, becoming as anachronistic and absurd, a phrase as plugging my toaster into the electric grid or something.
Bruce Schneier:	00:04:53	That's right, and that's what's changing, is the internet is becoming everything and we're seeing that with these Internet of Things. Traditional computers are screens we stare at,

		laptops and phones. That's all gonna be the old way of interacting with computers. They'll be embedded in our lives. They'll be our cars, our thermostats, our refrigerators, medical devices. They'll be toys. They'll be just things in our world.
Bruce Schneier:	00:05:22	And what I say in the book is that everything is becoming a computer, that it's no longer things with the computers in them, it's computers with things attached to them. So your refrigerator is a computer that keeps things cold, and your microwave oven is a computer that makes things hot, and an ATM machine is just a computer with money inside. And when you think about it that way, you start realizing that computer security becomes everything security and your car is just a computer with four wheels in an engine, which means it can be hacked, you can have ransomware on it, you can have malware. All of those computer things can now affect your car and I'm not sure we're ready for that.
Demetri Kofinas:	00:06:06	I was at a talk recently where Tim O'Reilly was speaking, who had been on the show not long ago, and he uses this metaphor of this like ecology or this ecosystem, and we're actually just increasingly part of this super organism and that's how he talks about it. Do you think of it that way? Do you think of the internet in that manner?
Bruce Schneier:	00:06:23	Yeah. I read his book and I didn't use his terminology, that felt too big and complex. I do use a term called the "Internet Plus." Now I hate inventing a term, none of us like it.
Demetri Kofinas:	00:06:36	Why the internet plus?
Bruce Schneier:	00:06:38	Because I wanted to encompass everything. There's the internet and we would talk about the Internet of Things, which is the internet of objects, but there's no word for the internet, plus the Internet of Things, plus the computers, plus the connections, plus the data stores, plus the services, plus the massive infrastructures like power plants, all connected, all this one big socio-technical system. There isn't a term for that, so I was stuck.
Bruce Schneier:	00:07:03	I mean, I could either use all of that phrase every time or just shorten it and I kept saying internet plus this, plus that, plus that, ended up with internet plus. I don't know if it'll stick. The last thing we want are more terms.
Demetri Kofinas:	00:07:17	But basically the idea being that everything that is connected is part of this internet.

Bruce Schneier:	00:07:21	And everything affects everything else.
Demetri Kofinas:	00:07:24	So one of the things that you do in the book and it's not the first time you've done it, you lay out these seven or eight aspects about the internet and connected devices and computers that make them particularly vulnerable or exposed. I think that it would be helpful for people that aren't familiar to run through some of those like, number one, software sucks, why does it suck? Also, the fact that these are these devices are multi-purpose, and that they're all connected, and the complexity that arises from that connectivity. Can you walk us through some of those things so people can sort of begin to understand why an internet of connected computers is vulnerable?
Bruce Schneier:	00:07:59	Sure, and I call these sort of lessons of computer security or truisms about computers that will be true about everything everywhere. The first, one as you say, that most software isn't very good. Basically, we don't want to pay for quality software. So, good, fast, cheap, pick any two, the market has picked fast and cheap over good, or fast and feature-rich over good. We don't want to pay what it would cost to make quality software with minor exceptions, like Avionics and the Space Shuttle, but other than that, most software is really poor. Poor software is full of bugs, some bugs are also vulnerabilities, some vulnerabilities are also exploitable, which means modern software is full of exploitable vulnerabilities and that's not going to change anytime soon.
Bruce Schneier:	00:08:49	The second one is that the internet was never designed with security in mind and it sounds crazy when I say it. But when you go back to the late '70s and early '80s, there were two things that were true. One, the internet was not used for anything important ever and two, you had to be a member of a research institution to get access to it. So, the designers really believed they could exclude bad actors because they just wouldn't have access to the mainframe you needed to get on the internet. Coupled with the fact that who cares? Deliberate decisions were made to ignore security, let the endpoints handle it, and we're still living with the effects of that decision.
Demetri Kofinas:	00:09:36	That security was not built into the network and that the nodes of the network could be responsible for managing their own security.
Bruce Schneier:	00:09:42	That's right, and the network was deliberately designed to be insecure because why bother? The third one you mentioned and the way I say it now is extensibility, so computer property. Basically means you can't constrain the functionality of a

computer because it's software. When I was a kid, I had a telephone at home, big black thing attached to the wall, a great device, but it can't ever be anything other than a telephone.

Bruce Schneier: 00:10:12 That iPhone is a computer that makes phone calls. It can do anything you want. Remember the slogan, "There's an app for that." An iPhone is fundamentally extensible, which means it's very hard to test because you don't know what's gonna do and you could attackers can change the functionality, put malware on it, put a virus on it, put ransomware on it in a way that's just in possible if it wasn't a computer, and I don't think most people understand that to that level.

Bruce Schneier: 00:10:43 Third lesson is about complexity, just complex systems are very hard to secure. I mean, that's the fourth, I might be running out of my numbers. Another one is that there are new vulnerabilities in interconnections and this is also a weird one, that as we connect things to each other vulnerabilities in one thing affects something else.

Bruce Schneier: 00:11:02 So 2016, the Dyn botnet, these were vulnerabilities in webcams and digital video recorders. Allowed a hacker to create a botnet that dropped a name server, that dropped a couple of dozen popular websites. Or some years before the target operation hack, the hackers got into the target payments network through a vulnerability in the HVAC contractor of several mid-Pennsylvania stores.

Demetri Kofinas: 00:11:31 So just to sort of clarify, that the idea behind that is that as you connect ... You can connect a bunch of other systems that would otherwise be secure in themselves but when you put them together, you can create an insecure network.

Bruce Schneier: 00:11:42 Or you can create an insecurity that is more catastrophic. So, earlier this year ... There is a casino in Vegas, but I actually don't know the name. They had their High Roller database, very sensitive formation stolen through a vulnerability, and I wish I was making this up, through their internet connected fish tank. That's how the hackers got in. So fish tank manufacturers are now critical to the financial health of companies that use their products and that's something we're not used to and we don't expect.

Demetri Kofinas: 00:12:14 Would it be a stretch to say that an analogy to that would be, if you've got five roommates and they all have keys to the apartment, and one of them is sloppy and he leaves the keys to the apartment on the coffee table in the coffee house near the apartment, and someone takes the key and gets into the

		building, each one of those other people can be secure, but when you put them all together, one piece of the components creates a larger insecure network?
Bruce Schneier:	00:12:36	Yeah. You can have stuff like that. There's examples where the way Google treats email addresses. I don't know if you know this, but in your Gmail address, the dots don't matter. So bruceschneier@gmail.com is the exact same thing as bruce.schneier, but a dot after every character goes to the same email box. Google just ignores dots.
Demetri Kofinas:	00:12:55	That's so interesting and I've heard you say that.
Bruce Schneier:	00:12:56	I mean, they do. That's just their policy. That's the way they design email address, the dots don't matter.
Demetri Kofinas:	00:13:01	They're anti-dot.
Bruce Schneier:	00:13:02	But if you have a service, and the way I saw this successfully done was against Netflix where the dots do matter. Now, you've got a system where Netflix thinks these addresses are unique, Google thinks they're common, and there are ways you can use that, basically, to hack Netflix.
Demetri Kofinas:	00:13:20	That's a great example.
Bruce Schneier:	00:13:21	Now, who's wrong? Nobody's wrong. It's a different way to think of email addresses, but if you put them together ... We saw this in the early days of seeing parts of credit card numbers. Now you know when you get a receipt, you don't have the credit card right, it's not like the last four digits. Though it used to be, before everyone set on the last four digits, it might've been some middle digital. It might have been the last digits. You collect enough receipts and you've got the whole credit card number, who's at fault? Nobody is. But the fact that they're doing it differently, means the whole credit card number's revealed.
Bruce Schneier:	00:13:54	There's a lot of that sort of thing on the internet and as we connect all these systems, I think we're going to see more and more of those sorts of things. There's a paper I just saw a couple of days ago. So the idea of this paper is that major appliances which draw a lot of electricity, think of refrigerators and think of air conditioners. If you can hack them, you could cycle the power in them in synchronization. And if you can do that, you can affect the load on the local power plant and cause blackouts.

Demetri Kofinas:	00:14:29	Wow. That's fascinating.
Bruce Schneier:	00:14:32	Now, I never thought of that, but as soon as I say it, you'd say, "Well, yeah, that makes a lot of sense. That seems obvious."
Demetri Kofinas:	00:14:37	And there are people that literally spent all day trying to figure out how to exploit these systems.
Bruce Schneier:	00:14:42	Yes. For all sorts of reasons, right? Ranging from countries' militaries to kids trying to figure out cool things to do after school one day, and everybody in between.
Demetri Kofinas:	00:14:52	So I don't want to derail us. I think the next one you were going to say on this list had to do with the all or nothing, basically. The way computers fail. They fail very differently than other devices or other components of our society.
Bruce Schneier:	00:15:02	So this is actually important. So you think about ... Let's take a car, we know how cars fail. Cars have parts, parts have these meantime engine failures and we could probably plot that a car will fail every X days, every X hours, so we can build repair shops to fix them. Computers fail differently. They all work perfectly until one day when none of them do and that kind of ... We call it class break in computers, a vulnerability's discovered in Microsoft Windows, or in PDF files, or on your Chrome browser and suddenly, it's insecure and they're all insecure.
Bruce Schneier:	00:15:38	So we saw this with hotel locks. There's a company, I forget their name, that makes those key card entry systems for hotels and it has a vulnerability. And now that their vulnerability is known, every single key card lock on the planet is insecure. Someone can break into the hotel room and the way to fix them is to go manually from door to door, which means it just won't happen. That is a failure mode that you don't see in a mechanical lock, and this is really the title, right? Click here to kill everything. It's not everything, but it's going to be all of a class of things.
Bruce Schneier:	00:16:19	Click here to open every door, click here to disable the brakes in every car or I guess, more realistically, every car have a certain make and model year, but that kind of class break is new for the rest of the world. We in computers have been dealing with it for decades.
Demetri Kofinas:	00:16:37	And the attacks are always improving. They're getting stronger and better.

Bruce Schneier:	00:16:40	Expertise flows down hills, is what I like to say, that today's top-secret NSA program becomes tomorrow's Ph.D. thesis, the next day's hacker tool. And we do see this again and again, that decisions we make at one time and we make them based on, "This technology is hard." Fast forward 10 years, we have the same decision, but now the technology is easy and cheap.
Demetri Kofinas:	00:17:01	And the philosophy in software engineering is very different than the philosophy and traditional engineering. Like, if you're a Rolls Royce in your building jet engines, you better get it right the first time. Whereas in software engineering, the idea is move fast and break things.
Bruce Schneier:	00:17:14	Or more, be agile, it's probably a better way to say it.
Demetri Kofinas:	00:17:18	And beta test.
Bruce Schneier:	00:17:19	So think about the two ways, there's the get it right the first time, which comes in the world of dangerous things: cars, planes, pharmaceuticals, and that's the world of testing, and licensing, and certification. Get it right the first time because the costs of failure are so great. Then there's the idea from the world of complicated and heretofore benign software, which is fix it quickly. That's the world of patching that we know we can't secure it, but if I can push a patch out within days or hours, that's almost as good. And those two worlds, I think, are colliding in software in cars, in medical devices, in voting machines.
Demetri Kofinas:	00:18:07	So both what I said and what you just said, I think those intersect for a point that I mentioned to you before we started, which had to do with Schlieffen Plan, World War I. Before this interview started, I was thinking about ... First of all, I struggle with this topic probably more than anything else we've ever covered on the show. We've devoted one episode to it. Obviously, there are all sorts of reasons that I struggled with it, but I was trying to figure out why, in particular, because we've covered a lot of really heavy topics.
Demetri Kofinas:	00:18:33	And I think the reason why is because unlike, let's say, global warming or any other sort of complex topic, there is no mental model that the public has to work off of. So when the news media talks about this, when they tell you NotPetya, they know NotPetya attack, or WannaCry, or Equifax, or Ashley Madison, whatever, they're telling you about all these different hacks, you don't have a way to put them into perspective. You don't have a way to get sort of an idea of where they reside.

Demetri Kofinas:	00:18:59	I was trying to think along those lines of an analog or a historical example, and I've seen a lot of panels where people bring up World War II, really, in the context of the atomic bomb, but that never felt right. And I mentioned to you, I was thinking along the lines of World War I because during World War I, we had a multipolar world, so there wasn't this bipolar world where diplomacy was easy. It was very difficult. In fact, Woodrow Wilson had a hell of a time trying to put together the League of Nations.
Demetri Kofinas:	00:19:27	And before World War I started, we had this huge industrial revolution and we had all this heavy artillery, so we had this new technology and there was what was known as the cult of offense. And the Schlieffen Plan with the generals put together in Germany was, based on this idea that mobilization mattered, whoever mobilized first had an advantage.
Demetri Kofinas:	00:19:45	And you made this point to me that not only is this true in cybersecurity, in the world of cyber, it's even more true because the weapons themselves, they have a half-life. They diminish over time. What do you think of that analogy and is there some way to help the audience, and listeners, and me as well, think about the severity of the threat and the precariousness of the situation?
Bruce Schneier:	00:20:09	Now the metaphors are hard because computers are different and they're not like anything else. I mean, just watch them play GO and you know they're just not human. So a lot of the human metaphors fail. I think I've had enough years with computers that telling people it's a computer, has some resonance as a core thing. But I think that some of our issue that we're trying to put this in human terms, but they really don't apply.
Bruce Schneier:	00:20:39	So what we talked about with cyber weapons, it's a weird property of a cyber weapon that it decays in value because it relies on a vulnerability to fire. So if I have a cyber weapon, I'm going to make this up, that targets the Russian power grid, they might fix whatever vulnerability I'm exploiting, not because they know I have the weapon, because they fix it. And so I have this weapon here and sort of every day, I'm wondering, "Is it still good? Is it still good? Is this still good?" I'm pretty sure in four or five years of won't be good and that means I'm a little more likely to use it while I can because if I hold it too long, I lose the ability.
Bruce Schneier:	00:21:25	And Rob Axelrod, he's a political scientist at University of Michigan, has written some really good papers on the game theory of cyber-attack based on this notion, and it's not like

anything else, right? Your nuclear weapons don't get worse because you wait. So the same sorts of theories don't apply.

Bruce Schneier: 00:21:45 I think we get really stuck and this is unfortunate, we're trying to push this into old metaphors because then we get it really wrong. But I'm trying make point in the room is that, "Look, the computer is the metaphor." These are all computers now. You got to think of them like computers, not like something else."

Demetri Kofinas: 00:22:02 You know, that's a really good point. I was also thinking, it's also you discover vulnerabilities, and once you to discover a vulnerability, you discover not only for your enemy but for you because we're all running the same software, right? And then on top of that, it's almost kinda like arrows because if you shoot an arrow, you can go get it and then use it on somebody else. So once we use an exploit or once it's been used, it's out there, like NotPetya, right? That was derived from a previous attack that the Russian government used against the power grid or Ukraine.

Bruce Schneier: 00:22:27 So I forget about NotPetya. I think Stuxnet, that's a better example, right? Stuxnet was a cyber weapon design of the US and Israel, and fired against Iran, against the nuclear power, program very successful. And that code, after the weapon was fired, has been used by cybercriminals in their own stuff because yes, once I fire a weapon at you, you can now look at it and learn from it in a way that's not really possible with-

Demetri Kofinas: 00:22:53 It can evolve.

Bruce Schneier: 00:22:54 ... a missile and it can evolve. This is very much nation-state, but we worry about non-nation states as well. So Stuxnet was a government program and its code is being used by criminals, and you do see that again and again, you remember the attack against Sony in 2016?

Demetri Kofinas: 00:23:15 Mm-hmm (affirmative).

Bruce Schneier: 00:23:16 I mean, there's a legitimate debate amongst security professionals, whether that attack was launched by a nuclear power with a $20 billion of military budget or a couple of guys in a basement somewhere. It turns out it was North Korea, but it could have been a couple of guys in a basement somewhere. The attack against the DNC, turned out to be the Russians. It could have been some kid. There's nothing about the techniques that make them unique to state actors.

Demetri Kofinas:	00:23:42	So as we move forward in time, does the material difference of having a large budget mean less and does the difference between what constitutes cybercrime versus cyber terror, or cyberwar, is that really simply a matter of incentive or the way that you deploy the weapon versus the type of weapon you have?
Bruce Schneier:	00:24:02	I think you're right on both counts that there is a blurring between budget and capability. That's why Iran really liked cyberweapons because they get to project power far in excess of what power they have in land, sea, and air. They really have a disproportionate advantage. It's why an activist like's a cyber attack, really magnifies his power. So certainly there is this difference of the way cyber weapons work. What was the second of your question?
Demetri Kofinas:	00:24:36	The point was about the budgets, one, which I think you just answered. And the other one was that, well, and I think you answered it. The difference is not the actual weapon, it's the way you use it.
Bruce Schneier:	00:24:44	And that's right because now we are seeing a world where everyone has the same tools, the same techniques, against the same targets and you really can't tell them it's between the governments and the criminals, and the activists. It is their motivation. It might be what they do after they break in, but they can all use the same attack tools to accomplish their goals and we see that now.
Bruce Schneier:	00:25:09	I mean, countries that can't afford an NSA, or a GCHQ, or the Russian and Chinese equivalent, will just use criminal hacking tools to pretty decent effect and they're just using it for state government purposes, even though it's the same tools.
Demetri Kofinas:	00:25:26	So these like cyber or marketplaces, these online bazaars where people are able to buy exploits or by vulnerabilities, the access the vulnerabilities or information about vulnerabilities, do we have any idea or do you have any idea what they look like? Because I imagine that intelligence agencies are going to be in there looking to buy, looking to, not only at the same time purchased these exploits or vulnerabilities, but also identify bad actors and that's happening both ways, and in that milieu is there's also these criminals who are looking to purchase.
Bruce Schneier:	00:25:58	So it even more complex markets. We actually have major defense contractors that find vulnerabilities and sell them to the US, to the UK, to countries that we might call the good guys. I mean, this is part of the defense industry --

Demetri Kofinas:	00:26:13	So there are people actually mining for vulnerable.
Bruce Schneier:	00:26:15	Yes, and this is the defense industry. There are companies that sell attack tools that include vulnerabilities to third world countries that you probably don't want to have them, right? The Kazakhstan's, the Sudans, the Bolivias, and I call them cyberweapons arms manufacturers, and they do sell attack tools ...
Demetri Kofinas:	00:26:39	With the consent of the US government.
Bruce Schneier:	00:26:42	Probably not.
Demetri Kofinas:	00:26:43	... looking the other way.
Bruce Schneier:	00:26:44	I don't think any of them are American companies, but there are companies in the UK, in Italy, in Germany, so they are in western countries and they are selling too. Israel sells attack tools.
Demetri Kofinas:	00:26:53	It's like landmines.
Bruce Schneier:	00:26:55	Its weapons. It's weapons of cyberspace and so those companies are buying vulnerabilities from researchers. And then there is this kind of seedier market, sort of online, where criminals are buying and selling stuff. I mean, the good stuff goes for real money to the people who pay a lot of money.
Bruce Schneier:	00:27:16	The bottom of this, if you're truly moral, you can report the vulnerability to the company and get a bag bounty, probably an order of magnitude less than you'd get selling on the black market, but at least it will be used for evil. But yes, the vulnerability market is very complex and there are people who study this. So there's a lot of papers on how this market works. Yeah, it turns out if you find a good vulnerability in iPhone, it's worth a quarter of a million dollars. That's a secure device.
Demetri Kofinas:	00:27:45	Is it legal to sell that?
Bruce Schneier:	00:27:46	It is not illegal.
Demetri Kofinas:	00:27:48	It's not illegal. So you could theoretically find a vulnerability, have no terrorists bone in your body, you're just really great at discovering vulnerabilities and you have no idea what it's going be used for, but you know what? You don't care and you sell it, and you make let's say a few hundred thousand or a few million dollars over some period of time and that ends up being used in

		some exploit that attacks a series of countries or a series of companies and wrecks billions of dollars' worth of the damage.
Bruce Schneier:	00:28:13	That certainly could happen. More likely if you're selling to that kind of money, it's being used for surveillance. So it won't cause damage, dissidence in some country will be arrested and that'll be the result.
Demetri Kofinas:	00:28:26	So going back to your point about the fact that we're all running the same software, so if the NSA finds a vulnerability or purchases one, that vulnerability has an expiration date, as soon as it's used and it can be used not only by the NSA, but also by enemies of the NSA or enemies of the US. It's also so weird to even think about this stuff, right? Because it's like these aren't really cyberspace. They're no real borders. It almost feels ... Bruce, I don't want to get like to kind of woo here, but I think it almost feels like we're transcending the Westphalian nation-state order and we're moving into this new realm where it's really not clear who's the enemy and who's the good guy here.
Bruce Schneier:	00:29:06	And where non-state actors have state like power, which is actually very hard for international relations to deal with. We know how to deter governments. There's a lot of theory on that. Deterring a non-nation state group, whether it's a terrorist group or even just kind of protest group is much harder.
Demetri Kofinas:	00:29:25	How much of that has to do with attribution?
Bruce Schneier:	00:29:27	It's attribution's source capability. Even if you know a couple of guys in a basement in Nigeria did a cyber attack, you can't stop them. You can't get to them. There's no enforcement mechanism. So attribution's a part of it, but not a lot. We have the names of some of the Russian military officers who attacked the US election, so what?. Attribution isn't helping there. Yeah, we get to put their picture in the newspaper and they're probably embarrassed, but no one actually cares.
Demetri Kofinas:	00:29:57	Actually, I'm going to bring up another great quote of yours, I actually have it here. I love this one because I want you to help me make sense of this and for the audience as well. You have a quote that I've heard you use when talking about attribution and you say, "There are three types of attribution: I know you did it. I know you did it and I can prove to you that I know you did it, and I know you did it and I can prove to the world that you did it."

Bruce Schneier:	00:30:21	So this is actually, I think ... Let's use Sony cases, an example. So we know that North Korea attacked Sony, actually, we don't know that, the US government knows that and they have said, "Please, believe us, the evidence is classified." So it's that three levels of attribution. We, in the United States, could know that North Korea attacked Sony. We can have evidence, so we're going to show to North Koreans and say, "Look, here. Right here's my evidence. I know you did it, don't deny it."
Bruce Schneier:	00:30:54	But maybe I still don't want to tell the world because if I tell the world, I reveal capabilities that I don't want to reveal. One of the things that came out in The New York Times and one of the reasons we knew North Korea did it is we had a human asset inside North Korean governments that was feeding us information, that's very sensitive. And you can imagine a situation, let's say, and I'll make this up, we were able to read sort of all their computer networks or a video of the order saying, "Attack Sony" or something.
Bruce Schneier:	00:31:28	You don't want to reveal your sources and methods. So during the time, it's 2016, the US government is saying, "North Korea did it," and we in the security community, a lot of us, just don't believe them. That's ridiculous. It makes no sense. You have no evidence to. You're just playing with us, and the US government couldn't show us the evidence. So they have to rely on trust and if you trust the US government that they're not going to lie about attribution, then you believe them. If you don't, you say, "Show me proof," and the government says, "I'm sorry, we can't this."
Bruce Schneier:	00:32:05	That makes that a little bit difficult. There's also weird attribution gap going on and a lot of ways the United States is much better at attribution because we spy on most of the internet. So we know North Korea did it in a way that another country can't possibly know, and we know who did it in national security cases, like the Sony attack, in ways that we will never know in law enforcement cases. We don't have the same tools there.
Bruce Schneier:	00:32:37	So attribution is a very complicated issue. We're, on the one hand, very good at it when it comes to national security nation states and we can be really bad at it with who's sending you those trollish tweets and threatening to kill you and rape you. We have no idea who did that.
Demetri Kofinas:	00:32:58	How accurate are these pronouns, we? You played a great role ... Listeners may not know, but you helped The Guardian sort through a lot of the classified documents that came out of the

		Snowden leak, you've seen a lot of this stuff. It's confusing to me to talk about us versus them in this environment. I don't feel comfortable. I don't think anyone should feel comfortable with anyone having these types of capabilities, but we are where we are. I think that also is sort of a way of bringing us back to this theory of war or theory of conflict. What work is being done either at an agency level, or government level, or in the private sector to try and create a framework for navigating this landscape in a way that would be okay for all of us?
Bruce Schneier:	00:33:44	So I think you're right and I tend to use the word we expansively, and it really depends on what level you're looking. That the United States is made up of very complicated interests working against each other and it's not just the NSA or US Cyber Command in the military, it's also the big corporations, Facebook is not our friend. Google is not our friend. These companies are working against our interests, that's how they make their money. So you can use we expansively and then you realize that there's a lot of us versus them inside every we and then probably turtles all the way down. So, yes, I am using a shorthand here.
Bruce Schneier:	00:34:24	In the end, I think the internet does magnify power in a very real way and the powerful get more powerful through these technologies. I don't know sort of how this will shake out in the end. I mean, certainly, the internet is empowering for the not powerful, but it seems to be right now more empowering for the already powerful. And whether those are countries or corporations, we see that in lots of different ways.
Demetri Kofinas:	00:34:57	What work is being done that you know of, for creating a theory for dealing with this? Let's say at least if not holistically, then what about even on a state level, state to state?
Bruce Schneier:	00:35:07	There is a lot of theory. There was none for many years, no one could define what war and cyberspace would look like, let alone how it can be waged. How do you know when it starts, when it ends, who won? What are the rules? Are there any Geneva Convention-like norms that we should follow? Like, maybe don't hack their hospitals. But now there is a lot of research of discussion, something called the Tallinn Manual, which is a pretty good book on what war and cyberspace looks like.
Bruce Schneier:	00:35:40	It doesn't have any force of authority, but a lot of people point to that. There are conferences, NATO is doing a lot of work in this. There's theories, there's academic work. I teach at the Harvard Kennedy School, there are people thinking about this there. So there is a lot, it's still very much in flux. Obama had a

		doctrine of war and cyberspace that some of it was public, a lot of it was classified. We know Trump has made some changes in that, all of that's classified.
Bruce Schneier:	00:36:07	So there's a lot we don't know, but you move out of the secret world of governments and there's a lot of open work trying to figure this out. There's just no consensus. There are no norms. We have norms and conventional war. I mean, if you declare war on me and invade, we both know what that looks like. We don't really know what that looks like in cyberspace, so we have things like the Russians affect the US election, is that an act of war? Don't know.
Bruce Schneier:	00:36:35	The Russians attacked the Ukrainian power grid, North Korea attacked Sony, US and Israel attack Iran, Iran attacks the Saudi national oil company. I mean, these are all happening, and it's kind of in this gray zone between war and peace because we haven't all agreed where the line is yet.
Demetri Kofinas:	00:36:57	I heard, Ash Carter, who's the defense secretary under Obama. I've heard him and I've heard a bunch of other people give different answers to what constitutes a cyber attack.
Bruce Schneier:	00:37:06	That's right. There isn't a broad agreement of what constitutes cyber attack.
Demetri Kofinas:	00:37:09	It's just wild. It's frightening, and also it's frightening in the context of the current breakdown in diplomacy. I mean, things are worse between the United States and Russia since anytime I remember. I don't know what the relationship is between the US and China at a deep sort of diplomatic level, there is a lot of grandstanding. I don't know if it's gotten worse. Certainly, the Chinese have been putting out lots of signals for years that they intent on continuing to exercise more power externally. So, I mean, have you heard in your circles, if the governments are in back channels communicating about this stuff?
Bruce Schneier:	00:37:44	I don't know. There are these more academic meetings were countries that might not be hostile are talking about this at the theoretical level. We know that Russia tried to penetrate power plants in United States. Now, we don't want that to be an active war because we do that too. Remember this story when a China attacked OPM, the Office of Personnel Management?
Demetri Kofinas:	00:38:08	Right.

Bruce Schneier:	00:38:08	Stole the personnel records of 20 million American government employees and you had James Clapper, who was the director of national intelligence in front of Congress. Some Congressperson said, "We were attacked," and he goes, "No, no, this is not an attack, sir, because we do it too." General Hayden used to run the NSA. He's a commentator on television now. He said, "I would have done that in a minute." So that isn't believed and treated as normal peacetime intelligence operations and not an attack. It might seem crazy, but that is the way we treat that.
Demetri Kofinas:	00:38:47	So this also highlights a problem, which is that Twitter technologically enable diplomacy through twitter. This is like with Donald Trump, President Trump who uses twitter freely, and what if he just tweeted, for example, that we were just attacked, "This is a cyber attack," or something like that? My point is that in every way on every level there seems to be a total confusion and these are weapons of mass destruction. You know a lot better than I have, but I've studied this as much as I can. I read also Ted Koppel's book years ago about shutting down the power grid and what that would look like. I mean, his worst-case scenarios or like horrific.
Bruce Schneier:	00:39:26	Yeah, that book has a lot of fiction and have a lot of reality.
Demetri Kofinas:	00:39:28	Has a lot of holes in it.
Bruce Schneier:	00:39:29	I think that-
Demetri Kofinas:	00:39:30	But is that not ... I mean, like even you write about this stuff. I mean, your book is called ... The third scenario is Click Here to Kill Everybody, which we should talk about by the way.
Bruce Schneier:	00:39:38	I think Trump and Twitter is less twitter and more the unfiltered Trump.
Demetri Kofinas:	00:39:44	Yeah, but the fact that he's able to do that ...
Bruce Schneier:	00:39:46	But he could have done that by holding a press conference. Pre-Twitter age ... You could have used the radio. It's more the words than the medium.
Demetri Kofinas:	00:39:56	You don't think it makes it a lot easier. I think you can subvert-
Bruce Schneier:	00:39:58	I think it makes it a lot easier.
Demetri Kofinas:	00:39:59	There's no impulse control.

Bruce Schneier:	00:40:01	But that's the person, not the medium. So an example of one which surprised me, at one point, Trump tweeted something about the US pulling families-
Demetri Kofinas:	00:40:13	The troops out of North Korea. Yeah, the families and the troops.
Bruce Schneier:	00:40:15	Right. I'm sure he was just saying that, not realizing that if you are a student of international relations that North Korea is going to take that as, "We are attacking you soon." Because we're pulling our families out because we don't want to put them in danger. Now, my guess is he didn't realize that that was the signal he was sending. That's not twitter, that's him.
Demetri Kofinas:	00:40:36	But Elon Musk also supposedly tweeted out something ... He was tweeting out about the Saudi deal when he was on Ambien. What I'm just trying to say is that shit happens.
Bruce Schneier:	00:40:44	But again, that's the person. I am not going to blame Twitter for that. I mean, Twitter makes it easy to draft a tweet.
Demetri Kofinas:	00:40:51	Hey, look, I am not exculpating Donald Trump for his tweets-
Bruce Schneier:	00:40:55	Or Elon Musk for his.
Demetri Kofinas:	00:40:56	... or Elon musk for his, not at all. What I'm saying is that there's a complimentary intersection here which is that we're on hair trigger. It feels like these things, I don't know what word to use, it just feels like things are at a more fragile state than they've ever been, than I can remember.
Bruce Schneier:	00:41:13	I mean, this is moving out of my area of expertise. This is really the social dynamics of social media and lots of people are studying that. My expertise is much more in the technical security of the systems, but certainly, people are writing about social media and how it either augments or diminishes certain types of conversations, and definitely, those are real social forces right now.
Demetri Kofinas:	00:41:40	We'll cover that too on the show. It just came off naturally. It wasn't something that I had thought about beforehand. It just feels like it's all sort of part of this thing which also can torch our sense of reality. The world, we're sitting here trying to describe, what is a cyber war looked like? I don't know. What does it look like? These aren't like bombs, and yet you could have a shutdown of a power grid or communication, and how will that affect diplomacy? And the picture you paint here isn't very

		pretty, right? I mean, the second to worst example is the one with the cars with shutting off all the breaks and that's something that you can do right now.
Bruce Schneier:	00:42:09	That's right. If you want to watch it, there's a great video on YouTube.
Demetri Kofinas:	00:42:12	I've seen it.
Bruce Schneier:	00:42:13	It's a reporter and he's in a car driving on a highway and there's a hacker 10 miles away with a computer, and hacker takes over the car. First, I think turns on the radio then turns on the wipers, and then disables the brakes.
Demetri Kofinas:	00:42:29	You can take the ransomware principle and use it for cars, right?
Bruce Schneier:	00:42:31	That's right and it will happen, right? You'll wake up in the morning, you go to your car and your car won't start unless you pay $2 of bitcoin, and we just hope it doesn't happen at speed.
Demetri Kofinas:	00:42:39	What if you're in the car and you're parked and an autonomous car decides to drive you to the terrorists, and like you can't keep-
Bruce Schneier:	00:42:46	Or even drive you to Seattle, right? This car is going to Seattle unless you-
Demetri Kofinas:	00:42:51	How much is it worth for you --
Bruce Schneier:	00:42:52	-- not to go to Seattle. I like Seattle but, you know ...
Demetri Kofinas:	00:42:55	Seattle is nice. The West Coast is nice, but look, I'm making light of it. I'm laughing out of awkwardness, to be honest with you, it's awkward. This is so freaky to read about it and there's so many problems that we're encountering, whether we're talking about global warming, whether we're talking about the traditional weapons of war. There are all sorts of issues that we're facing, economic, and there's so much dysfunction. This brings us back to this point that technology is augmenting that dysfunction. It's augmenting it.
Bruce Schneier:	00:43:22	And the part I write about sort of in here is this world of physically capable of computers, that unlike the computers of last year, today's computers can do stuff. They turn on the power, they steer your car, they fire your pacemaker, and these physically capable of computers are sort of fundamentally much more dangerous. It used to be about data and now it's about life

		and property and that's what I think the difference is. That's what I'm writing about. This is a much more dangerous world because we've given computers hands and feet. We've given them the ability to affect the world in a direct physical manner.
Demetri Kofinas:	00:44:03	Before we get into some sort of solutions because you've proposed them in the book, what are we looking at over the next few years? These attacks have been growing in scale, right? As we move along the vector of time, what can we reasonably expect to see over the next few years?
Bruce Schneier:	00:44:20	I think the same sorts of attacks we see against computers and phones against other things. It's a ransomware, ransomware against your refrigerator, ransomware against your car. We know that computers dragoons to botnets, and these are thousands or millions of computers that can all be synchronized to attack something on the internet. And we're starting to see things being dragooned into botnets, we'll see more of that.
Bruce Schneier:	00:44:45	We are seeing more attacks against large-scale systems and the ones you worry about are gonna be the power grid, the financial network communications network, these are vulnerable. Already FinCEN is trying to grapple what a catastrophic attack it the infrastructure of this country would look like and how to recover from it. So people are thinking about this. When I look at the trends, that's what I look at. In addition to some of the more conventional crimes, some of the ways to steal money, ways to harm someone happening more over computers.
Demetri Kofinas:	00:45:22	But where is the sclerosis here? For example, there have been some companies like Merck. What's the name of the company that was hit with a NotPetya attack?
Bruce Schneier:	00:45:30	That's Merck.
Demetri Kofinas:	00:45:30	So, yeah, 10-
Bruce Schneier:	00:45:31	I heard $300 million.
Demetri Kofinas:	00:45:33	No, you're right. The total scale was 10 billion for all the companies affected or people affected, and there was, of course, the Sony attack. There are lots of companies-
Bruce Schneier:	00:45:41	FedEx was hit by-
Demetri Kofinas:	00:45:42	FedEx was hit.

Bruce Schneier:	00:45:42	... NotPetya, a very extensive one.
Demetri Kofinas:	00:45:44	So corporations don't want to spend money on their own security, they would be happy to lobby the government to do it. Where is the problem here that we're not getting some comprehensive regulatory approach to deal with this? And on top of that, our company starting to get the message because not petty apparently did not have good security practices. Equifax was obviously a horrific case. They actually redirected people to the site. They send the amount of the pan into the fire, what's going on? Is it the same forces of political sclerosis that we're seeing across the-
Bruce Schneier:	00:46:14	It's a couple of things. It's mostly the tech industry doesn't want to be regulated. Let's use Equifax as an example. We just had the first anniversary of the Equifax attack, I was one of the people who testified before the house after Equifax and I gave a pretty scathing testimony, and they were Congress-people on both sides of the political aisle who are angry and lots of strong words and, "We must do something about this." It's a year later and nothing happened, not even a little thing. Nothing. Zero, no change. Equifax didn't matter, right?
Bruce Schneier:	00:46:48	They're not even our customers, we can't even fire Equifax. Nothing changed and I think that is exemplary. That's what happens. Nothing has changed about Facebook and probably won't. Lots of strong words. So a couple things going on here, these companies are incredible financial engines for our country and nobody wants to touch that. Nobody wants to break that.
Bruce Schneier:	00:47:17	Silicon Valley was built on this very strong libertarian government "Get out of my way" mentality and polled pretty much sway and then there's sort of the unwillingness to deal with it, both on the government level and on the corporate level. I'm not convinced FedEx did a whole lot. The market really doesn't reward good security, it rewards mediocre security and taking the chance.
Demetri Kofinas:	00:47:47	I want to actually make a point here because this brings us back to the point, I forget how you frame it when you talk about it, but we talked about it earlier, where a system is only as secure as it's most insecure component, right? So the traditional rules of laissez-faire economics don't apply here because if we're all using the internet, you can't simply have everyone just take care of this at the node level, right? That's not going to be enough, right? Obviously, you made the point, the internet was not built with security in mind, but at the end of the day, there are things we can do at a high level.

Bruce Schneier:	00:48:20	There's a lot we can do it and this is my point of interconnectedness, that we're making everything that is one big system and now vulnerabilities here can effect here. Vulnerabilities in that inner connected air conditioner that you just bought can drop your power grid, that's bad. Vulnerabilities in your fish tank can affect your financial network, that's bad. And I think we're not really fully understanding the effects of that. Now there is this rush to connect it all.
Demetri Kofinas:	00:48:54	Forget about it. I've had so many arguments with my father about this, he's connected so much shit, totally unnecessary.
Bruce Schneier:	00:49:00	But it's going to happen and-
Demetri Kofinas:	00:49:01	Totally unnecessary.
Bruce Schneier:	00:49:02	Yeah, but that's not going to be the answer. And I think this is actually worth explaining that the reason everything will be internet connected is because it will be cheaper than not, because it used to be if you are a plights manufacturer and designing the refrigerator, it would have some kind of circuit board. It would be a specially made dedicated circuit board to run that refrigerator and it's all it could do. Today, it is much cheaper to pull a general computer chip off the shelf and write some software, and stick it on the chip, and put it in your refrigerator.
Bruce Schneier:	00:49:35	And that means that refrigerator is much more powerful than it has to be, and it comes with internet connectivity. It comes with video drivers. It comes with speakers and a microphone, all those things. It's there. So you're an engineer saying, "Well, what the hell? I might as well use it," it's here, and now that you have all this functionality, you invent reasons for it and my guess is there will be enormous benefits in internet interconnecting everything that we just can't imagine, that they did these emergent properties. But I'm talking about the security downside, but it's usually not your father who's right about technology, usually, it's your kids, but in your case, you've got it backwards, but he's right.
Demetri Kofinas:	00:50:16	He was always pretty advanced on these stuff.
Bruce Schneier:	00:50:18	The connecting everything is our future. I don't think we can sort of back our way out of it, we have to forward our way out of it.

Demetri Kofinas:	00:50:26	So just so you know, though, his IoT devices were used as part of a botnet attack against Sony devices worldwide. Just so you know, we found out about it. They had to get shut down by the ISP.
Bruce Schneier:	00:50:39	Oh, had it shut.
Demetri Kofinas:	00:50:39	They had to shut it down.
Bruce Schneier:	00:50:41	And most times you don't actually know. You might have a digital video recorder that's part of the botnet or any of the dozens of other botnets use same vulnerabilities, you stare at the thing, you have no way of telling. I mean, oddly, you kind of don't care.
Demetri Kofinas:	00:50:55	So what can we do? Like, what are the best ways forward on this? What is it that we can do either at a national level, or at a local government level, at a corporate level, or at a personal level? How do we manage this?
Bruce Schneier:	00:51:08	My book is primarily about policy and I think the problem we have is lack of policy. It's not really lack of tech, there is a lot of tech we can deploy but we choose not to because the business case isn't there. And I think what's missing is government and I spent a lot of time about how that might look like, different ways to have liabilities, and standards, and regulations, and court system, and things that regular wages can do, international treaties.
Bruce Schneier:	00:51:39	There's no single answer. There's no, "Do this one thing and you'll be safe," it's going to be a whole menagerie of different things. And just like any other industry, I think we will approve slowly. Again, just like any other industry, but the missing part of the equation has been government, that government has largely stayed out of the tech sector, and what I argue in the book is that's no longer tenable, that that worked when it didn't matter, that worked when it was just data.
Demetri Kofinas:	00:52:09	And money.
Bruce Schneier:	00:52:10	Right. But when it becomes life and property, governments will get involved. Governments regulate things that kill people and there is no industry in the past 150 years, longer, that has improved that safety and security without being forced by government: cars, planes, pharmaceuticals, medical devices, consumer goods, workplace safety, food production, restaurants, most recently financial products. The market

		rewards doing a mediocre job and taking your chances. If we want better, we have to demand it.
Demetri Kofinas:	00:52:54	But it's even worse than that because it's not even a situation, in many cases, like Equifax where the customer is the one who's at risk. It's actually the product, you are the product. They're using our data to sell to their customers, so they're even less incentive.
Bruce Schneier:	00:53:11	Right. They're an extreme case because we can't fire Equifax and we didn't even know they had our data, so they have no incentive to protect it. A more marginal case is Facebook where, again, we are their product and in theory, we can choose not to use Facebook. I know lots of people who hate Facebook but are on Facebook because, socially, they have no choice, that Facebook is a monopoly in that space and people are kind of stuck on the platform because otherwise, they don't find out about their friends' lives or parties they get invited to.
Bruce Schneier:	00:53:41	In my book, I talk about surveillance capitalism as one of the drivers of this, these are these companies that are spying on us in exchange for services and how they're not working on interest and they're working against security. There is also now an architecture of control that we're starting to see, that it used to be a company would sell you a book and then it's your book. You can do whatever you want with it. A company like Norton sell this book, they can't stop me from doing anything with this book I want.
Demetri Kofinas:	00:54:05	You can throw it at your spouse.
Bruce Schneier:	00:54:06	Throw it at my spouse. I can sell it to somebody else, I could photocopy pages, but if I buy this book on a kindle, it's very different. A kindle can decide whether I can lend that book to you. Kindle can decide whether or not I can do text to speech, some books I can't, some books I can. They might say, "You can have a typeface larger than this, smaller than that. You can't read the book slowly or in automobile.
Demetri Kofinas:	00:54:33	DRM.
Bruce Schneier:	00:54:34	DRM, but more for devices. Auto manufacturers want to sell you a car that if you don't make your payments, it automatically shuts off. When a coffee houses buy those high-end espresso machines, they come with computers that are monitoring usage to upsell products, deliver spare parts. You bought this coffee machine, but you didn't buy the latte feature, you can only

		make this kind of coffee, can't make that kind of coffee. John Deere does that with tractors, farmers cannot repair their own tractors because the license of the software doesn't allow that.
Bruce Schneier:	00:55:12	So it's DRM, but it's about physical capabilities for objects you think your own now. I think that's a problem for a business perspective, but it's a security problem as well because as soon as there's a capability to shut off your car remotely, I don't have to worry about who can push that button and they want just the bank to be able to, but what if the bad guys can too? As soon as that button exists, you have a security problem.
Demetri Kofinas:	00:55:41	So I think actually now we're starting to get closer to what I was trying to get at, which is there's this just incongruence between the reality, and the technology, and our mental models and the relationship to things. Cars are a classic example, if you're not the driver anymore, how does liability work? What does it mean to get into an accident? How does all this stuff work? And I feel like we're starting to collide in this area and we haven't developed a model or even begun to develop some type of framework for thinking or talking about this stuff.
Bruce Schneier:	00:56:09	And yet we are rushing headlong into that future.
Demetri Kofinas:	00:56:11	Right. So does that mean that we have to have some existential crisis? There has to be some huge loss of life, like a 9/11 or worse in order to get the government to actually act? And then, what does the government acting under duress look like in the scenario?
Bruce Schneier:	00:56:26	So I think the answer is bad in both cases. I think governments are terrible being proactive.
Demetri Kofinas:	00:56:32	Is this why you live in Minnesota, Bruce?
Bruce Schneier:	00:56:33	It's much more complicated reasons. I think that it will take a crisis that governments aren't motivated unless the real thing happens, something bad happens, that they're not going to be proactive about it because the companies don't want it and they're going to successfully lobby. I think we do need to have some serious thinking. I think we're reaching a point where tech is moving faster than policy, or conception, or mental models and we've never lived inside like that before. What does agile government looked like? We don't actually know.
Demetri Kofinas:	00:57:04	I think there's a contradiction in terms ...

Bruce Schneier:	00:57:05	Yeah. But it can't be anymore. I think it is, but it can't be because when we're living in a world where advances in AI are happening as fast as they are today, we better figure out what the algorithmic discrimination looks like, and what it means, and what's legal, and what isn't, and what do we do when software makes the decision but cannot explain itself? Is that good? Is that bad? Do we like-
Demetri Kofinas:	00:57:29	Like the black box.
Bruce Schneier:	00:57:30	The black box, but if it's a better decision, maybe we like it, but how do we know what's better? What does better mean? And these are all very deep questions. They are bigger than security, but security is a lot of these questions.
Demetri Kofinas:	00:57:43	Our presidential elections exacerbate this, I think, the fact that we get so obsessed with their electing our president and we don't really pay much attention to local politics, for example, but is that the wrong way to think about it? Should we start to think more locally? Does that mean that local governments and states are going to have more power versus the federal government and that we need to look to nonprofits and other types of approaches?
Bruce Schneier:	00:58:05	I think I've looked everywhere. I mean, right now in regulation and cyberspace, I look at two places: I look at the states, most notably New York, Massachusetts, California, who were doing a lot of good work and I'm looking to Europe, right? The EU is now the regulatory superpower on the planet and they are not afraid to flex their muscle. So we just saw a massive privacy law. You know, in the past few months, you've been seeing a lot more warnings on websites, that's because of Europe and they're going to turn their attention to security and safety next.
Bruce Schneier:	00:58:36	So that's where we're going to see change. These are global problems, I think, that are parts of solution at every level of government, but the sort of, the neat thing about some of these solutions is that we'll benefit regardless.
Bruce Schneier:	00:58:52	So I'm going to make this up. There are toys that are interconnected. The Norwegian, the Tumor Council of all people did a study of some of these dolls and they had enormous security violations. They were declared illegal by the German government because they are surveillance devices and these companies actually improve their security because they couldn't sell these dolls in Germany and in Europe. Now that improved dolls also sold in the US.

Bruce Schneier:	00:59:19	The company's not going to maintain two different software products because it doesn't make any sense. So Europe has some good regulations and we benefit. Now compare that to something like Facebook that very much was going to want to have two different products. Figure out people who are subject to European privacy law and people who are not because they'll get more profit out of the ones who are not. But when you get to physically capable computers and safety, I think we will benefit if you're a past law or if California passes the law, and sort of both ends of the size spectrum.
Demetri Kofinas:	00:59:50	Well, I don't want to poo-poo those things, but they seem to be marginal. They seem to be on the margin that, like the stuff that you write about in the book that you've written about for years, that just seems to be like the frightening majority of the concerns that I have. When I look at that, we've talked about this during the course of the show, that still leaves me with the question of, "Do we need to have some huge loss of life? Do we need to have some crazy, scary experience to motivate the public to demand that the government ends up doing something, but what does that look like?"
Bruce Schneier:	01:00:23	So the answer, unfortunately, is probably. We as a society are terrible at being proactive, that it does take a disaster to motivate people, especially when you have a lot of lobbying interests saying, "Don't do it. Don't do it. Don't touch it. Don't disturb it. It's making money. Leave us alone," it's going to take a disaster. One of the reasons I wrote the book is to start having this discussion about what good regulation looks like before the disaster because you know what happens after disaster.
Bruce Schneier:	01:00:54	Government says something must be done, this is something, therefore we must do it and he gets something stupid. If we can, now when we have the luxury of time and calm, figure out what a good regulatory regime looks like, when the crisis happens, if the government says, "What do you got?" We can say, "Don't worry, we've spent the last 10 years thinking about it, here's what you should do." And we're going to get parts of it wrong, but it's better than acting completely out of fear.
Demetri Kofinas:	01:01:24	It's also problematic though because Apple, for example, has a lot of business overseas. So, what happens if the US decides that China has attacked it? Now it says in order to accommodate for these existential crisis, we need to impose draconian measures against Apple, which now we'll screw it's business sort of oversee. The interconnectivity of all this, it just feels like ... I just don't know how that's supposed to work.

Bruce Schneier:	01:01:51	We have theories of commandeering and we know what that looks like for the government to say to Chrysler, "Stop building cars, start building tanks." There's real hostility. I mean, not just, Cold War fake hostility but actual military hostilities. We know how to go to Apple and say, "You're now doing this," and Apple says yes because it's extraordinary times. I don't think that's going to happen. I'm not-
Demetri Kofinas:	01:02:14	The commandeering did happen though at a time where we didn't have globalization in the same way that we have now.
Bruce Schneier:	01:02:18	That's right.
Demetri Kofinas:	01:02:19	Is Apple a US company? I mean, it is, but how much is it a US company?
Bruce Schneier:	01:02:23	... Irish company?
Demetri Kofinas:	01:02:24	Exactly.
Bruce Schneier:	01:02:25	But that's when you can have to declare your loyalties. When there's war going on, there's no room for, "Well, I'm not really a US company." Look, "You are or not. If you're not, leave. If you are, we now are going to take over your network because we actually need it."
Demetri Kofinas:	01:02:39	Really confusing.
Bruce Schneier:	01:02:40	To me, this seem pretty farfetched. I worry a lot more about normal time.
Demetri Kofinas:	01:02:46	Well, Bruce, I don't want to take up any more of your time, so I want to thank you for coming on the show. Let me grabbed the book here. Let's give everyone a view of this book again, Click Here to ... just don't click there, actually. There's no actual place that people can actually click here, right?
Bruce Schneier:	01:02:58	No, no, that is just real website.
Demetri Kofinas:	01:02:59	It's just a book cover.
Bruce Schneier:	01:03:00	That is just a book cover.
Demetri Kofinas:	01:03:01	Just a book cover and I'm sure they can get that on Amazon. And then if people want to follow you on Twitter, how do they do that?

Bruce Schneier:	01:03:07	I think I'm Schneier Blog on Twitter.
Demetri Kofinas:	01:03:08	Schneier Blog.
Bruce Schneier:	01:03:09	Yeah. I blog on schneier.com, and that's where I write all my stuff. And it is mirrored on Twitter, it is mirrored on Facebook. You just search for Bruce Schneier, you'll find the various places to find me.
Demetri Kofinas:	01:03:19	I told you I think I've been subscribed to your newsletter since 2007. I don't think it's changed. The website hasn't changed since then, has it?
Bruce Schneier:	01:03:24	No, it's pretty much old school.
Demetri Kofinas:	01:03:26	It's pretty old school.
Bruce Schneier:	01:03:27	It has changed a little bit. I think I tend to run a decade behind.
Demetri Kofinas:	01:03:30	You started it ... When did you say? Nineteen ninety?
Bruce Schneier:	01:03:32	I think I started it in 1997. It's been about 20 years.
Demetri Kofinas:	01:03:35	Amazing. Well, I really appreciate you coming on the show. It was great having you.
Bruce Schneier:	01:03:38	Thanks for having me, this was fun.
Demetri Kofinas:	01:03:40	And that was my episode with Bruce Schneier. I want to thank Bruce for being on my program. Today's episode of Hidden Forces was recorded at Edge Studio in New York City. For more information about this week's episode, or if you want easy access to related programming, visit our website at hiddenforces.io and subscribe to our free email list.
Demetri Kofinas:	01:04:03	If you're a regular listener to the show, take a moment to review us on Apple Podcasts. Each review helps more people find the show and join our amazing community. Today's episode was produced by me and edited by Stylianos Nicolaou. For more episodes, you can check out our website at hiddenforces.io. Join the conversation at Facebook, Twitter, and Instagram @hiddenforcespod, or send me an email. As always, thanks for listening. We'll see you next week.