Demetri Kofinas: 00:00 The Hidden Forces Podcast features long-form conversations broken into two parts, the second hour of which is made available to our premium subscribers, along with transcripts and notes to each conversation. For more information about how to access the episode overtimes, transcripts, and rundowns, head over to patreon.com/hiddenforces. You can also sign up to our mailing list at hiddenforces.io, follow us on Twitter, @hiddenforcespod, and leave us a review on Apple Podcasts. And with that, please enjoy this week's episode.

Demetri Kofinas: 00:54 What's up, everybody? My name is Demetri Kofinas and you're listening to Hidden Forces, a podcast that helps investors, entrepreneurs and everyday citizens get an edge by equipping themselves with the knowledge needed to anticipate the challenges and opportunities of tomorrow. By sharing my critical thinking approach and by challenging consensus narratives about the power structures shaping our world, I help you make the connections to see the bigger picture, empowering you to make smarter decisions.

Demetri Kofinas: 01:28 On this week's episode, I speak with Nicole Perlroth, award-winning cybersecurity journalist for The New York Times and author of a recently published book on the cyber-weapons arms race, titled "This Is How They Tell Me The World Ends." This is the latest episode in a series that I have devoted entirely to the subject of information security and to the growing threat posed to our infrastructure and to our lives by the exploitation of vulnerabilities in our software and connected devices.

Demetri Kofinas: 02:00 Cyber-attacks against individuals, companies and infrastructure have increased steadily year after year. Attacks, like the recent one targeting a water treatment facility in Florida or the SolarWinds hack discovered last December and which compromised thousands of private and government users, including Homeland Security, The Pentagon, and the NSA, are only the tip of the iceberg. The reality is that these attacks are going on 24 hours a day, seven days a week and the cost that they impose both to individuals and organizations are measured in the trillions of dollars every single year. My objective in bringing you this conversation is to highlight both the nature and the urgency of the threat posed by the cyber-weapons industry and the flourishing market for exploits and vulnerabilities, and what measures we can take to protect ourselves both individually and most importantly, as a society. So, without any further ado, here is my conversation with journalist and author, Nicole Perlroth.

Demetri Kofinas: 03:15 Nicole Perlroth, welcome to Hidden Forces.

Nicole Perlroth: 03:19 Thanks for having me, Demetri.

Demetri Kofinas: 03:21 It's my pleasure to have you on. So, where are you speaking to us from?

Nicole Perlroth: 03:25 I am actually talking to you from Lake Tahoe. I usually live in the Bay Area, but we had a pipe burst, so we are staying in our cabin in the woods and it's actually where I wrote the book, so it's nice to be back here.

Demetri Kofinas: 03:39 I was speaking with someone about this. I saw on your bio that you actually went out of your way to point out that you love spending time in your cabin in the woods, and it kind of makes sense, I feel like, because if I were covering the kind of crazy stuff that you look into, I'd want as little connection to the outside world as possible.

Nicole Perlroth: 04:00 Yeah, it was such a nice place to get away. I have a two-year-old, so I needed to get out of the house to do this. And being somewhere where all I really had was a really bad internet connection, but no smart devices, no Alexa's, no Google Homes, no Sonos' even, was pretty comforting, given what I was writing about.

Demetri Kofinas: 04:25 So I'd love for you to tell me and our listeners how you got into this. First of all, what got you started in journalism? Is that how you found your way into this field or did you have an interest in cybersecurity before you became a journalist?

Nicole Perlroth: 04:39 No. So, I had never been a journalist in school, I'd never had a byline. I went to Princeton. And I always enjoyed writing and I always enjoyed story-telling and I loved reading. And I took all these jobs after Princeton that Princeton grads take, I worked as a consultant for a while, I was a paralegal, when I thought I might want to go to law school, I worked at Coach, the handbag company, in marketing for a while. And each job was just more mind-numbing than the last, to me. So, I actually took this course in continuing adult studies at NYU when I was living in Manhattan and it was in writing, I just wanted to do something that was a little intellectually stimulating at night. And the guy who taught the course was this guy named John Crudele, who was a longtime business columnist for The New York Post, and he pulled me aside one night and said, "I think you have something here. I think you should try freelance journalism." And you might even remember this, it was the week that they had discovered these rats doing cartwheels in the back of a Taco Bell/KFC in the West Village.

Demetri Kofinas: 05:50 Oh, yeah, I do remember that. I actually know that Taco Bell very well.

Nicole Perlroth: 05:55 Yes. Yes, so did I.

Demetri Kofinas: 05:56 I lived right by it.

Nicole Perlroth: 05:56 So did I. And I lived right by it too. So he said, "Why don't you do a story on all of these really well-respected restaurants in Manhattan and their health records, and you can talk about how the Taco Bell/KFC's not the only one with rat problems?" So I said, "Okay, I'll try this." So I went and I looked through the Department of Health records and I found this abysmal restaurant health report for this restaurant I had just eaten at in Chelsea. I don't even remember the name. But it was a delightful restaurant and I couldn't imagine them having the cockroaches and rat feces that were listed on this report. So I went and walked there after work, after my day job at Coach, and I said, "What is up with this health report? It says you guys have this huge rat infestation, but I was just here and I loved your food and everyone seemed great and diligent." And they said, "Oh, yeah, that guy came, he got drunk at the bar, he passed out on the bar for a couple hours and then to justify why it took him two, three hours to do the inspection, he failed us on everything and we actually have footage of it, here you go."

Nicole Perlroth: 07:05 And so I went back to The New York Post and I said, "I'm so sorry I didn't do the assignment you gave me, but I did get this video footage of this health inspector drunk, passed out at the bar at this restaurant that he failed." And they just laughed at me and were like, "You have no idea what you just got." They put it on the front page of Sunday's post with this amazing headline, it said something like, "Rat Nap, Inspector Snoozeau," and then there was my name, by Nicole

Perlroth. I don't even remember, I think I wrote one paragraph of it. And I was sold. I remember I went to the bodega that weekend and I bought up every New York Post they had and I was just totally addicted to journalism.

Nicole Perlroth: 07:48 I ended up going to journalism school and I went to Stanford, they have a little program. And one of the things that was cool about going there is you could take these courses at some of the other schools, so I took this class there in bioethics, it was sort of the business of the biology, pharmaceutical industry, the business ethics of it. And we had this guy come in, talking about how they were trying to develop a new birth control and all of the sort of ethical wrangling that he had to go through to decide do we have to pay people who end up getting pregnant in this study, do we have to pay for them to get an abortion? Do we have to pay for their kids' college education if they end up having the kid? How are we going to handle this? And I'd never thought about how many moral decisions are involved in business.

Nicole Perlroth: 08:40 And so while everyone in that journalism class wanted to go cover politics and the arts and music, I thought, wow, I would love to cover business and the ethics of business. And so that turned into an internship at Forbes Magazine and ultimately, a job there. And story by story, started getting a little more high profile and I was covering venture capital right at the peak of the private market for Facebook and Twitter stock, and these VCs seemed like celebrities. And I was writing cover stories about people like Peter Thiel and Jim Breyer, who'd invested early in Facebook, and The Times caught notice of me and that was around 2009, 2010. So they called and they said, "We have a job for you we're looking at you for, but we're not sure you're going to want it, given the topic." And I said, "Well, how bad could it be? You're The New York Times, I'll probably take whatever you offer me." And they said, "It's cybersecurity," and I just had to sigh and say, "Not only do I not know anything about cybersecurity, I've actually gone out of my way not to know anything about cybersecurity."

Demetri Kofinas: 09:50 Interesting.

Nicole Perlroth: 09:50 So-

Demetri Kofinas: 09:50 Why is that? What do you mean, you went out of your way?

Nicole Perlroth: 09:53 Well, it just seemed so terrifying and a little bit boring, to be honest, compared to what I was covering in Silicon Valley, and I thought you want to take me off this gravy train, covering venture capital as it's just picking up and these companies that they're investing in are just having these sky-high evaluations and this is all anyone wants to talk about, and no-one wants to talk about cybersecurity. And not only that, but there were a lot of people I knew who covered cybersecurity really well, not just at Forbes, but elsewhere. And so I essentially told The Times that in my interviews, I said, "Here are some people, here are some names for people who are excellent cybersecurity journalists," at my interview and they said, "No, no, no, you don't understand. We've interviewed all of them and we had no idea what they were talking about."

Demetri Kofinas: 10:39 Interesting.

Nicole Perlroth: 10:41 So what they really wanted was a translator. They wanted someone who could immerse themselves in cybersecurity, in some of these very technical issues and translate them for the lay audience. And so I took the job and I told myself, maybe if I do cybersecurity really well for a couple years, they'll let me go back to venture capital. And the first big thing that happened was The Times got hacked itself by China, and so it really threw me into the deep end. And I basically embedded with our security team and the FBI and Mandiant, which is now FireEye, the company that just flagged this giant Russian hack on our federal IT networks for several months. We didn't publicize the attack until we knew we had eradicated the hackers. So, for several months, I got a big front row seat to what a nation state attack on a private company looks like, and in that case, it was my own employers and I ultimately wrote about it.

Demetri Kofinas: 11:38 Hmm. Well, I can't wait to get into that. I'm curious, how different is this beat and the characters, also, incidentally, how different are the characters covering cybersecurity versus what you covered in business?

Nicole Perlroth: 11:55 Well, the thing that is the same is it's a largely male-dominated space with several notable exceptions there. It is filled with egos, many of whom bruise easily. It is hypertechnical. And the thing about covering cybersecurity ... Or sometimes people correct me and say, "It's not cybersecurity, it's information security," which I talk about in the book a little bit. The thing about covering it is that the people involved in these issues are a very special breed. They have been calling out cyber threats for years and years, if not decades, and they have been ignored, so they come at this with a little bit of a chip on their shoulder. They also, and rightfully, in my opinion, treat these issues like religious issues. Sometimes, I just want to sit down with our Israeli, Palestinian conflict reporter to just try and compare notes about who gets more flack on Twitter. Because in their mind, what they're saying-

Demetri Kofinas: 12:57 Interesting.

Nicole Perlroth: 12:58 Is if we don't take this seriously, we're going to have the equivalent of a terrorist attack or we're not going to have privacy anymore. They've been calling those things out for years and years and years, and they've been ignored. So when you finally reach them, they're almost screaming at you and a lot of them get very upset with The New York Times and mainstream publications that haven't been covering these issues in the way they believe they should be covered, which is almost like a religious issue to them. So it's a hard, hard, hard audience to satisfy, especially when you're writing for a general audience.

Demetri Kofinas: 13:37 Yeah. I saw that you deleted your Twitter account-

Nicole Perlroth: 13:41 Mm-hmm (affirmative).

Demetri Kofinas: 13:41 Just a few days ago. What's that about?

Nicole Perlroth: 13:43 Well, it wasn't one thing. I've been on Twitter for 13 years, I signed up right when I started doing journalism. And back then, it was sort of like this VC clubhouse, actually. It's interesting now that Clubhouse is taking off. It was just a few celebrity venture capitalists, like Fred Wilson, kind of walking us through their philosophies on investing and startups, and you could really have a conversation with people. But over the last decade, it has just become such a place of vitriol, a place where you can't really have a real conversation in a lot of cases. I think there's a lot of humor and snark that brings some joy to my daily life. But I had decided, at a certain point, if this starts feeling more destructive than it is beneficial to my journalism, to my life, to my mental health, I will leave. And that is essentially what happened.

Nicole Perlroth: 14:43 I was actually listening to Sacha Baron Cohen do a podcast the other day and what he said was that there's not actually free speech on Twitter anymore because there are so many troll armies or just people who act like trolls, who just jump at whatever you say, that it actually silences a lot of people, particularly women and minorities. And I felt like I was logging onto Twitter every day and there'd be a new name sitting in the trending topics column that everyone was mad at that day, and there was nothing-

Demetri Kofinas: 15:17 Totally.

Nicole Perlroth: 15:17 That person could say to quell everyone's anger, and it just bothered me. And when my book came out, what started happening was ... And I knew writing a book on this subject matter, I would be kicking the hornet's nest and I knew that actually, if I didn't kick the hornet's nest, then I wouldn't have done my job. But what started happening, and I sort of predicted this, but what started happening is people would screenshot paragraphs of my book out of context and say, "This is wrong," or "This is xenophobic," or "Defend yourself on the spot." And this book is easy to take out of context because it is the story of a market, it's the story of the rise of global warfare, but it's also this first person story of my own learning journey and I'm a different person at the end of the book than I am at the beginning of the book.

Demetri Kofinas: 16:13 Don't you know, Nicole, that you're not allowed to change, you're not allowed to have any kind of maturity-

Nicole Perlroth: 16:17 No.

Demetri Kofinas: 16:17 Experiences.

Nicole Perlroth: 16:17 No.

Demetri Kofinas: 16:18 And everything you've ever done, you have to be held accountable for right now.

Nicole Perlroth: 16:22 Yes, exactly. And so that's what it felt like. And I tried to respond to some of it, but any response just engenders more anger, more trolls, more people who are calling me all sorts of names. And I found myself, to be totally honest, just in a fetal position last week and I just thought, why am I trying so hard to survive or prove to myself I can survive this toxicity? The next day, I realized I had not been present for my two-year-old at bath time and I'd snapped at my husband and I was just sort of irritated, and I realized it wasn't anything they were doing, it was Twitter. And so I just fired off that last tweet and said, "Don't let the bastards get you down and be kind to one another, and follow me on this website and reach out to me on LinkedIn and see you."

Demetri Kofinas: 17:18 Ah, man. We've all been there. Oh, man.

Nicole Perlroth: 17:26 There's that GIF or GIF, whatever we're calling it these days, of Angela Bassett in the movie, Waiting to Exhale, where she lights the car on fire and walks away. That's sort of what I felt like.

Demetri Kofinas: 17:37 I could totally see you with your husband, on your phone, sucked into this horrible universe and then just snapping.

Nicole Perlroth: 17:43 Yeah.

Demetri Kofinas: 17:43 We've all been there. Yeah. And Twitter's also a disinformation platform.

Nicole Perlroth: 17:48 Yes. Yes.

Demetri Kofinas: 17:48 It's a place where active measures are constantly running.

Nicole Perlroth: 17:52 Yes. And I've been a target of those. I've had Russia Today write stories and take my tweets out of context and call me racist or whatever they said that day, and it was very clear that there was a nation state element to some of these charges. And what do you do, as a person on Twitter with a life and a mom of a two-year-old, defending yourself from these troll armies? It's just gotten impossible.

Demetri Kofinas: 18:17 Yeah. No, it's super scary, especially when you begin to challenge power and platforms like Twitter. Even if you aren't hacked ... And I'm curious, we'll get into all that, how you manage security. But in any case, it's super scary and it takes some level of courage to do this. So I mentioned I've read your book, obviously, fantastic book. Lovely cover, I've got to say, beautiful artwork on the cover.

Nicole Perlroth: 18:42 Oh, thank you. Thank you. Yeah, it's hard. I was scared that they were going to come up with something like explosions and bombs and cyber, cyber, and I'm really glad that they went really simple.

Demetri Kofinas: 18:53 Yeah, it's beautiful, actually. I'm a huge fan of judging books by their cover, so great job. The book is called This Is How They Tell Me The World Ends: The Cyber Weapons Arms Race. I guess, the question I have to start off is how does the world end? How did you get this title? How did this come about?

Nicole Perlroth: 19:12 Well, it's funny, I love doing this because I can actually answer the question not in sound bites. But I got this notepad that you can write on in the shower, I don't know where I found it, but I put it in my shower when I was living, in my 20s, by myself and I just started taking notes in the shower on if I wrote a book, what would it be called, and what would the chapter headings be called? And one day, I just found myself writing down, "This Is How They Tell Me The World Ends," in the shower. And it's because when I started on this beat, and, again, I was very green when I came into this, every conversation I had with a government official or someone in industry seemed to end with this warning that we were due for a cyber Pearl Harbor, some kind of calamitous, cyber-induced, kinetic attack that would take out the grid or a nuclear plant or water treatment facility and cause deaths. And they said, "Until we have that happen, no-one will take this seriously."

Nicole Perlroth: 20:16 And it was almost comical because I would ask these people, "Okay, well, how long do you think until this attack's going to happen?" And without fail, they all had the same answer, it was always, "18 to 24 months. 18 to 24 months." Just long enough that it might actually happen, but also just so far enough in the distant future that if it didn't happen, I might not hold them to it. And it's now been something like 100-something months since they started telling me that. And so my opinion about this has changed and, like I said, this book was a learning journey. On the one hand, I don't like the analogy cyber Pearl Harbor because we didn't see those planes coming, whereas we have been talking about the cyber equivalent now for decades.

Demetri Kofinas: 20:59 We didn't see the Japanese planes coming, you mean?

Nicole Perlroth: 21:01 Yes, exactly. And we have seen something like the cyber equivalent coming for a very long time. And the second thing is I think it's a distraction from where we already are, which is all of our intellectual property has been targeted and, in many cases, stolen by China. We have seen Iranian hackers mucking around the controls of American dams. We have seen Russia break into our nuclear plants and power plants. And in one case, there was this famous screenshot that Homeland Security released of Russian hackers literally with their fingers on the switches at a power plant. We have seen our hospitals get locked up with ransomware, and we've seen some of that come a nation state or two nation states, actually, North Korea and Russia. And we've seen Russia turn off the lights and power to Ukraine a couple times.

Nicole Perlroth: 21:52 So, every attack that I've covered over the past decade has been a slightly deadlier or more costly attack than the last, and I do think we are headed for some kind of cataclysmic attack. Now, what that would look like, it could be one attack on the grid, but, in my opinion, it's probably going to be something more coordinated, like an attack on the grid combined with an attack that might contaminate our water supply, like the one we saw attempted in Florida the other week, when a hacker upped the level of lye, L-Y-E, in the water to a nearly deadly effect. And then ransomware on our hospitals that would keep doctors and nurses from treating patients. If you could detonate all of those things at once, it would look a lot like what we just saw in Texas the other week, when the power went out and the water got contaminated, only they might keep the power off and prevent people from going to the hospital, that kind of thing.

Demetri Kofinas: 22:53 So, so many thoughts. I first began studying cyber-attacks well before I actually started Hidden Forces, so sometime before 2017. And I remember one of the books that I had read in that process was Ted Koppel's Lights Out. I think that was the name of the book.

Nicole Perlroth: 23:11 Great book.

Demetri Kofinas: 23:12 Great book. And I think you actually cited it at one point in your own book because you referenced the duration of how long the grid could potentially be compromised. And I remember-

Nicole Perlroth: 23:22 Yes.

Demetri Kofinas: 23:22 Reading in Koppel's book that depending on what parts of the grid are attacked, it could take two years to restart the system because of how long it takes to construct some of those pieces.

Nicole Perlroth: 23:34 Mm-hmm (affirmative).

Demetri Kofinas: 23:35 So ... Yeah. I mean, the scale of the potential damage is enormous, that's one observation. Another thing that came to mind when you talk about hospitals, hospitals, for me, were the thing that sort of brought to light the significance, the ease with which our systems can be attacked.

Nicole Perlroth: 23:54 Mm-hmm (affirmative).

Demetri Kofinas: 23:54 I mean, power grids, everyone kind of gets that. But I did an episode, it was Episode Eight with Josh Corman, and I think he had said there that, in referencing kind of large-scale attacks, that up until now, we've been measuring the damage from cyber-attacks in dollars and cents, but at some point, we're going to begin to measure them in terms of flesh and blood. And-

Nicole Perlroth: 24:16 Wow.

Demetri Kofinas: 24:17 What I learned there about hospital systems ... I mean, I don't know ... I'm curious what you have to say on this, but my recollection was that 70 percent or some large number of hospitals don't even have a dedicated IT person or a firewall and that because of the Affordable Care Act, I think, and HIPAA regulations, so many of these hospital systems had started putting all their medical devices online, like MRI machines and everything else.

Nicole Perlroth: 24:46 Mm-hmm (affirmative).

Demetri Kofinas: 24:46 And one really simple attack that he talked to me about was just scrambling blood records in the morning, so right before patients go into surgery, people start dying and no-one knows why. So one immediate question that comes out of that is ... Well, before I even ask that, here's a question for you. What do you think most people in the U.S., and then, I guess, I don't know how people's impressions of this threat change outside the United States, but what are most people's impressions of what cybersecurity is, of what the threat of cyber-attacks are, and what a cyber-attack itself is, the nature of it versus what is the actual reality?

Nicole Perlroth: 25:30 Mm-hmm (affirmative). Well, I think for a long time, people's only real experience with a cyber-attack was ... And there's a huge discussion about whether even to call these cyber-attacks or hacks, so let's just stick with hack because people have very strong feelings about this. But most people's experience with this is their identity was stolen or their credit card was used for fraud and there was no real repercussions to it. Your bank would pay you back if someone stole your credit card information. Your personal information, that could take a bit longer to sort out and it was more of a headache. But people didn't really understand that there were deeper repercussions for attacks, and those deeper repercussions come from the fact that we are hooking up the internet of things at a rate of something like 127 new devices per second. When I say devices, I mean things like pacemakers, insulin pumps, baby monitors, cars, railways and increasingly, our critical infrastructure, power grid, our nuclear plants. And that means that all of those digitized access points can be exploited by hackers for something more nefarious.

Nicole Perlroth: 26:53 Now, the hospital analogy is a good one. And I really don't like to overhype the threat because then, I think, people's eyes roll into the back of their heads and they feel hopeless. But the reality is we are starting to see these attacks or hacks play out in a way that is becoming very dangerous. So just recently, I covered an attack on a Vermont hospital with my colleague, Ellen Barry, where they were hit by ransomware, probably by cyber criminals. And when we talked to the nurses, they said, "No-one knows how bad this is. The only thing I can compare it to in my career is working the burn unit after the Boston Marathon bombing."

Demetri Kofinas: 27:35 Wow.

Nicole Perlroth: 27:36 Yeah. And they said, "It wasn't just that we couldn't access people's patient records, it's that cancer patients couldn't get their chemotherapy because these are really complicated protocols and we have complicated records documenting who has gotten what, and all of that was erased." And so, suddenly, these nurses in the cancer unit were forced to try to remember everyone's chemo protocol from memory and in some cases, they just couldn't recall it and people weren't getting their infusions. So, this is hitting us in a way that I think people are really starting to feel it.

Nicole Perlroth: 28:14 And the attack the other week in Florida is just such a good example of this. Here's this town, just ahead of the Superbowl, just outside Tampa, population, 15,000, hackers got into their controls, upped the level of lye in their water and had that drinking water made its way to people's taps, that would've sent everyone to the hospital when these hospitals are already under siege from the pandemic. And then you're talking about a potentially serious life-threatening situation. And if you combine that with a ransomware attack on that hospital, that could really be deadly.

Nicole Perlroth: 28:57 But that is what is happening. These attacks are getting more visceral for people. And for so long, like I said, people were saying, "We have to wait for that cyber Pearl Harbor before people wake up and do something." And what I would like to say right now is-

Demetri Kofinas: 29:13 Interesting.

Nicole Perlroth: 29:14 We don't have to wait for that attack because it's already so bad and people are starting to feel it, let's do something before we have that really calamitous attack.

Demetri Kofinas: 29:26 Yeah. So, again, a lot of thoughts. One is just the interconnectivity of everything.

Nicole Perlroth: 29:31 Mm-hmm (affirmative).

Demetri Kofinas: 29:32 You mentioned how the context of the larger pandemic within which this was happening. You can press on one area or pull one thread and tons of other areas of our modern economy and society get affected.

Nicole Perlroth: 29:47 Yeah. Yes. And I think that, to me, is the least understood part of this, that we are so interconnected. I actually think the pandemic might end up being one of the best things that happened to our awareness of cyber threats because it's a good analogy. I mean, you can't really see it until it touches you, and the same thing is happening in cyber. You can't really see this threat, it's invisible, it's playing out in code that many of us can't read or don't understand at all and you don't feel it until it touches you, until you have to go to the hospital and they turn you away because they've been held up with ransomware, or because your lights go off because hackers just turned them off from Russia, or because they unleash the controls at a dam. You don't feel it until it touches you.

Nicole Perlroth: 30:36 But we are all so interconnected, so much interconnectivity and complexity has been added to our digital infrastructure and to our lives. We all bought into it because we were promised this sort of frictionless Silicon Valley, frictionless society where we could access anything from our phones, not just Ubers, but the controls at an oil rig or water treatment facility remotely. But all of that access can and increasingly has been exploited by hackers.

Demetri Kofinas: 31:10 Yeah. I think the way that it was presented and perhaps continues to be presented is that it's all upside. Just connect your Jeep-

Nicole Perlroth: 31:17 Right.

Demetri Kofinas: 31:17 Cherokee to the Cloud.

Nicole Perlroth: 31:18 Yes.

Demetri Kofinas: 31:18 Connect your thermostat. It's just all upside. But there's clearly a security downside that people just didn't take seriously. I think it was Bruce Schneier, because we also did an episode with Bruce, I think it was Episode 60 or 60-something, uses this term or this phrase that we've always been vulnerable, it's just that now we're exposed because we've connected all of these devices that were always vulnerable, like our SCADA systems, the industrial control systems, to the internet. All of a sudden, systems that were never designed to be connected are connected and all of a sudden, all those vulnerabilities are exposed.

Demetri Kofinas: 31:52 So this might be a good opportunity, Nicole, to help people understand what a cyber-weapon is, when we're talking about vulnerabilities and exploits, with the aim, in part, of also, I think, educating people on just how easy it is to conduct one of these attacks with the right exploit.

Nicole Perlroth: 32:15 Yeah. So, I mean, there's a lot of debate about what a cyber-weapon is, but I think it's probably easiest to start with the most famous, which was Stuxnet, the attack that the U.S. and Israel pulled off on Iran's Natanz nuclear facility that used code to spin its uranium centrifuges out of control, in some cases, it slowed them down, and ultimately destroyed something like 1000 Iranian uranium centrifuges and did so with code. So that was a cyber-weapon of destruction, but it was incredibly careful. It was designed to only exact destruction on the exact configuration of centrifuges at Natanz nuclear facility. Now it got out, as most cyber-attacks do, it escaped the target, we don't know how, but that computer worm spread all over the world and hit companies, like Chevron in the United States. And it didn't do any destruction because, like I said, it was clearly built with the NSA's general counsel standing over someone's shoulder to make sure it was a very precise weapon, almost like a scalpel. But it showed what could be done in this realm.

Nicole Perlroth: 33:35 And since then, we have seen other nation states deploy code to exact destruction in much less careful ways. And the one that really comes to mind here is NotPetya, which is a terrible name for an attack that Russia detonated on Ukraine, which was basically a gigantic ransomware attack with no way for the ransomware victims to pay the ransom. It was not profit-seeking, its intent was just to paralyze Ukraine's government agencies and some of its critical infrastructure and companies. And it did that, but just like Stuxnet, it got out and it circled the globe, it hit Cadbury chocolate factories in Tasmania, it hit Pfizer, it hit Merck. Merck was ... Its vaccine production lines were paralyzed by that attack and it actually had to tap into the CDC's emergency stockpiles of Gardasil vaccines that year. This was 2017. And it hit Maersk, the shipping company and paralyzed global shipments.

Nicole Perlroth: 34:39 So, it had huge collateral damage. And it wasn't designed with the way Stuxnet was designed, it was not designed to be a scalpel, it was designed to exact destruction and as much destruction as possible in Ukraine and it got out and it did destruction elsewhere. But that is the problem is that the NSA and Israel pulled off this bloody masterpiece of an attack, it was fascinating to go back to the context in which they pulled off that attack. We had been getting pressure from the Israelis, some inside the NSA told me it was like a PSYOP, a psychological operation, to hand over bunker buster bombs. And every simulation that the Bush administration had done, The Pentagon, to see what would happen if we allowed Israel to bomb Natanz showed that we would be dragged into World War Three. This was 2006, 2007, when the death counts of American soldiers in Iraq was just going up and Bush had no appetite for getting into a third war in the Middle East, and so they went with this third option, which was Stuxnet, the computer worm that ultimately destroyed the centrifuges.

Nicole Perlroth: 35:49 And so, short-term, that was the digital equivalent of the Manhattan Project without the bombs. It saved lives, kept Israeli jets on the ground, setback Iran's nuclear ambitions a few years. Long-term, I think it's a legitimate question to ask whether it was beneficial because, now, Iran has really emerged from this very basic, unskilled cyber adversary into one of the most determined and prolific adversaries we now face in cyberspace. Their nuclear ambitions are back to where they were, without the Iran nuclear deal. And it also showed other countries that it was perfectly okay to reach into another nation's nuclear plant and take things out, so long as you did so with code. And increasingly, that's what we're seeing is these other nation states probe our systems with code, our critical infrastructure.

Demetri Kofinas: 36:46 Yeah. You called it a masterpiece. It was like the Sistine Chapel of cyber-attacks. Kim Zetter wrote a book, Countdown to Zero Day, for anyone who's interested in just-

Nicole Perlroth: 36:56 Excellent book.

Demetri Kofinas: 36:56 Yeah. I mean, it's remarkable. It was an air-gapped system, so they managed to basically, through a USB or maybe there was ... We don't know, unless-

Nicole Perlroth: 37:04 Right.

Demetri Kofinas: 37:05 I don't know if something's come out since. We don't know if someone was compromised and they introduced the virus into the system, but they entered the system through a Windows device and then eventually got it into their nuclear reactor systems, which ran Siemens. And then they-

Nicole Perlroth: 37:16 Mm-hmm (affirmative).

Demetri Kofinas: 37:17 If I remember correctly, they were toying with the system and incredibly intelligent.

Nicole Perlroth: 37:23 Yes.

Demetri Kofinas: 37:23 An incredibly intelligent virus that eventually, once it was found out, was even programmed to basically do as much damage as possible before it was shut down.

Nicole Perlroth: 37:31 Right. Yeah. First of all, as far as I know, it's the first time that attack jumped from Windows systems into the PLC systems, the industrial controllers that we use in factory floors and nuclear plants and power grids. And once it got in, it waited almost two weeks to make sure it was indeed the system that it intended to target. It was very careful. Like I said, it was definitely designed with lawyers' feedback in mind. And then what it did was it would speed up the speed of these rotors, which is the most fragile part of the uranium enrichment process, and then it would sit back for 27 days and do nothing. And then it would go back in and it would slow the rotors down and then it would sit back for 27 days.

Demetri Kofinas: 38:17 Incredible.

Nicole Perlroth: 38:18 And all the while, if an Iranian engineer was staring at his computer screen, everything looked like it was going smoothly. So they really did it in a way to make it appear like a natural accident. It was almost like a psychological operation to make them doubt their capabilities, to make them doubt that they had what it took to enrich their uranium.

Demetri Kofinas: 38:40 If I were to describe where you focus most of your attention in the book, well, it's heavily character-driven and a ton of attention is devoted to the cyber-arms market or trade.

Nicole Perlroth: 38:52 Mm-hmm (affirmative).

Demetri Kofinas: 38:53 How has this market evolved over the last X number of years? And how important is that economic component of all of this to the insecurity that we all face, globally?

Nicole Perlroth: 39:07 Well, the reason I focused on the exploit market, or the cyber-arms market, is I was fascinated by the incentive structures and I was fascinated by the moral hazard baked into this incentive structure. So just backing up, just because I don't think a lot of people even know what a zero-day is. If I find a vulnerability in your iPhone iOS software that Apple doesn't know about and no-one knows about that secret flaw in the code is called a zero-day. And if I'm a hacker and I can construct the code or the program to exploit that flaw to spy on your text messages or track your location or your contacts, your calendar appointments or turn on the audio on your iPhone without you knowing, I can sell that capability, that zero-day exploit to governments.

Nicole Perlroth: 40:01 And the going rate for that capability right now is about 2.5 million dollars, according to one U.S. broker's prices. And I learned about a new broker that just works for the Saudis and the Emiratis in the course of reporting out this book, but they'll pay even more, they'll pay something like three million dollars for that capability to remotely access your iPhone. And when they purchase that zero-day exploit, they have no interest in ever telling Apple about the flaw because that would turn their zero-day exploit to dust, essentially. As soon as a manufacturer, like Apple, learns about these flaws, they patch them, they roll out software updates, you install the software updates, then the flaw gets fixed and governments lose that access.

Nicole Perlroth: 40:48 So I was fascinated by the moral hazard there, because two, three decades ago, if we found a flaw in Russia's computer systems or in Huawei, the Chinese software company, hardware company, if we found a flaw in those systems and we used it to spy on Russians and Chinese, no harm, no foul because most Americans didn't use that technology or Huawei's routers and switches. That is not the case anymore. For the most part, we are all using iPhones or Android phones, Siemens software for industrial plants, or Schneider Electric. Whether you know it or not, you're using Microsoft Windows in your daily life. So when the government found a zero-day or acquired a zero-day exploit or developed a zero-day exploit in those systems and they did not tell Microsoft or Apple or Google about them, they were logically leaving Americans less safe by leaving that flaw open.

Nicole Perlroth: 41:48 And I knew, from my coverage over the last 10 years, that it was not a theoretical that cyber criminals or nation states would try to acquire and use those capabilities against us, they were doing so. They were clearly motivated to get into our critical infrastructure to spy on their own people, as was the case with the Emiratis, in attack after attack that I covered. And even in places like Mexico, I was covering these hacks and surveillance, using these zero-day exploits and spyware of journalists, of human rights lawyers, of activists. Even nutritionists, at one point, in Mexico, called me and we had discovered spyware on their phone. And I talked to a bunch of them and I thought, this is weird, why are nutritionists getting hit with government spyware? And low and behold, it was because what they all had in common is they all had been pushing for a soda tax in Mexico, so, clearly, someone in government was corrupt and didn't want that tax to pass and was getting kickbacks of some sort.

Nicole Perlroth: 42:50 And so what I saw was an unregulated marketplace dealing in our vulnerability and I saw that this code was making its way, increasingly, into our critical infrastructure and I saw where all this was headed, which was to a place I don't think any of us want to go, which is a place where anyone can acquire the capability to turn off the lights or to spy on and intimidate journalists and curtail free speech. So, that's why I focused there, but it also has all of these threads out to global cyber warfare and this capabilities gap that was steadily closing.

Demetri Kofinas: 43:29 So I have one question that came up very early on in your answer, which is what is the process like for finding a vulnerability?

Nicole Perlroth: 43:39 Mm-hmm (affirmative).

Demetri Kofinas: 43:41 What is required in order to do that? And then contrast that with developing an exploit for that vulnerability.

Nicole Perlroth: 43:47 So, here, I'll tell you that, again, I'm a translator, but I've never done this myself. So I did talk to a bunch of hackers for the book to flesh out these definitions and explanations. But, essentially, what it is, is you can test software any number of ways. You can throw junk traffic at it, you can go line by line, you can attack it with fuzz farms, which are these computers that just throw traffic at this code and wait to see which code holds up and which code falls apart, and then you can dig through the code that falls apart to find out where the flaws are. And when you find a flaw, you can just write a program, again, this is just in code, to exploit that flaw for any number of purposes. So, once you break that program, you've just written an exploit. And it could be something like I find a flaw in MP3s and I send you a MP3 music file and I've created the code to exploit it, so that when you click on that music file, I am inside your phone.

Demetri Kofinas: 44:58 So the SolarWinds hack that happened recently, that was a hack of a security software. Correct?

Nicole Perlroth: 45:05 It wasn't a security software, it was ... With SolarWinds ... And they had started marketing it as security software, which is a bit of a joke, now that we've dug into their security. The biggest nightmare that IT administrators face these days, now that we've all switched over to our personal devices and cloud applications, is that they have no idea what's going on in their network. So one of the main selling points for some of the software companies over the last decade has been we'll sell you software that gives you great visibility into your systems. You can see which cloud applications your employees have downloaded, you can see what they're doing on those cloud applications, you can see where your data is moving, whether it's to employees' personal iPhones and Androids or to Dropbox. It just gives them visibility into their networks. And a lot of governments and more than 400 of the Fortune 500 had downloaded and used the software, SolarWinds software, to get better visibility into their systems.

Nicole Perlroth: 46:08 Now, because it gave organizations such visibility, it also had a lot of access into the systems. And so what it was, was the low-hanging fruit that Russia used to access government agency systems and, in some cases, private company systems. And, essentially, they just back-doored the SolarWinds software update. So they got into the SolarWinds' build process and just as SolarWinds was going to release a software update to its customers, it did this last minute switcheroo, where instead of SolarWinds software update, you were getting a Russian Trojan horse.

Demetri Kofinas: 46:48 Interesting.

Nicole Perlroth: 46:49 And once that Russian Trojan horse was rolled out into SolarWinds' client systems, it could've potentially had access to the 18,000 organizations that downloaded this Russian Trojan horse. But what we see, and what we're starting to see as we unwind this attack, is that this was a targeted hit mainly on U.S. government agencies, but also companies like FireEye, which is one of the nation's premier security companies. And they stole some of FireEye's tools and we know they breached Microsoft and viewed its source code, and we know they got into some email security firms and we're still unwinding that attack.

Demetri Kofinas: 47:26 So the exploit was the update?

Nicole Perlroth: 47:30 Yes. They used the update as a backdoor into these systems, but the definitions get a little murky here-

Demetri Kofinas: 47:38 Right. I mean ... Sure.

Nicole Perlroth: 47:38 Because we don't know how they got into SolarWinds yet. We don't know-

Demetri Kofinas: 47:40 Right.

Nicole Perlroth: 47:40 If it was a zero-day exploit. Now what we're learning about SolarWinds is that their internal security was so poor, it would not have taken a zero-day exploit, they probably used something much more basic, like a phishing attack or ...

Demetri Kofinas: 47:52 Well, the reason I brought up SolarWinds and I was asking is because are there certain types of software or certain formats that hackers target to look for vulnerabilities over others? I mean, are there certain places where they spend most of their attention, that it's more fruitful to investigate?

Nicole Perlroth: 48:12 Well, every hacker has his or her own interests and so some of them ... And hacker, by the way, is often a misunderstood term. Really, it's just someone who has an interest in getting to the bottom of things, tinkering with them and seeing if they can use it for some alternate use. Some of the times, it's good, its benefits are security. Sometimes, black hats use it to steal money or nation states use it for espionage or destruction. So, in this case, hackers all over the world have their own interests. Some are really interested in anti-virus software. That is a very ripe target because when you think about it, anti-virus software has deep access to your machine because they have to scan everything as if it's a potential threat. So if you can get into or find a way to exploit anti-virus software to use it as a spy tool, you have tremendous access to someone's machine. You have access to every file on their computer, you have access to every application on their computer.

Nicole Perlroth: 49:18 And over the past decade, we've seen good hackers, that is hackers at Google, for instance, find these gaping holes in anti-virus software that could be used a spy tool. But some of the riper targets are things like Microsoft Windows just because it's so ubiquitous. iOS software, I already mentioned. If you can find a way to remotely exploit vulnerabilities in iOS software that would enable you to read someone's iPhone communications, if you're a spy, what else do you need? You have their location, you have their contacts, you have all of their communications, you have their surround sound. You can turn on their camera without them knowing, so that's a big one for governments, particularly governments that want to surveil their own people and keep tabs on journalists and that kind of thing.

Nicole Perlroth: 50:05 So it really just depends what do you want to spy on, or where do you want to look? And the problem is anywhere you look, there are vulnerabilities in software because at the end of the day, it's humans who write software and we're not perfect. So, we're constantly rolling new bugs into code and those bugs form the raw material for a lot of modern espionage programs.

Demetri Kofinas: 50:29 So why is deterrence so hard in cyberspace, and how does it compare to traditional deterrence in the analog world for normal military attacks?

Nicole Perlroth: 50:40 Mm-hmm (affirmative). Well, deterrence has worked with the nuclear analogy. If Russia were to detonate a bomb here, we would turn around and do the same to them and we know that and so no-one has actually gone ahead and done that. What's wrong with that analogy in cyber is that the barrier to entry is so much lower. You don't need fissile material for these tools, you just need a laptop and you need someone who has the skills to find vulnerabilities and exploit them and develop payloads for those systems that could do serious harm. On the other end, there's another problem, which is we, the United States, NSA and Cyber Command, we are constantly attacking or spying on these systems and we do so with code. So once we hit these systems, once our adversary discovers that code, they can unravel it, they can reverse-engineer it, they can retrofit it and they can use it back on us.

Nicole Perlroth: 51:41 There was an attack ... We don't know exactly whether it was the U.S. or Israel, but there was an attack some years ago on Iranian oil facilities that was wiping data on their networks, just destroying the data. And that was discovered and it was remediated. And less than three years later, Iran used this exact same mechanism, not necessarily the exact same code, but the same mechanism, to wipe out data at Saudi Aramco, the oil facility. And that time, they didn't just wipe out the code, they replaced it with an image of a burning American flag to send a message that they could do this too. So, that's why deterrence doesn't work. In cyber, the enemy is a very good teacher. You can learn from attacks on your own systems and you can turn it around.

Nicole Perlroth: 52:30 The other thing is it's a real asymmetrical playing field. We, the United States government, might hack other governments and their critical infrastructure, but a lot of our adversaries see that our crown jewel, here in the United States, is our economy. So after Iran pulled off that attack on Saudi Aramco, they came for our banks with a pretty basic attack called a denial-of-service attack that flooded these banks' websites with code and took them down, so Americans couldn't access online banking for a while. And it wasn't a calamitous attack, but it cost these banks millions, if not tens of millions or hundreds of millions of dollars, to remediate and protect themselves from. And so what we're seeing is that nation states have found that the private sector is big target for them, that they can actually do more damage to the United States by hacking our private sector than they could potentially by hacking the government.

Demetri Kofinas: 53:33 That's a really fascinating insight. So a couple of thoughts. One is, as you mentioned, this sort of evens the odds. Not only does it elevate the potency of nation state attacks from what we traditionally think of rogue nations or weaker developing countries, but it also elevates the status and capabilities of non-state actors.

Nicole Perlroth: 53:56 Yes. And that's another problem is some people, and the person who's been the leading voice on this is Brad Smith, the President at Microsoft, have advocated for a Digital Geneva Convention, where we nation states would all agree to not conduct cyber-attacks on infrastructure like hospitals or elections or the power grid. Okay, so on its face, that sounds delightful, right? Okay. But the problem is most of the attacks that come out of the United States on these other countries come out of Cyber Command these days and that's not the case in Russia and China and Iran.

Demetri Kofinas: 54:37 Attribution. The problem is attribution.

Nicole Perlroth: 54:39 Attribution. Yeah. And in Russia, we saw a couple years ago, Putin said, "Hackers are like artists. They just wake up in the morning and start painting." And, essentially, the implication was I have no control over them. Now, we know that's not true, but he has maintained a great deal of plausibility in these attacks. In Iran, we just saw these indictments when they indicted several Iranian hackers for some of their attacks here in the U.S.. A lot of those hackers didn't work directly for the state, they worked for front companies, for the IRGC. And in China, the most sophisticated attacks we see these days are not from the PLA, they're from the satellite network of contractors that get tapped on the shoulder by the Ministry of State Security that says you're coming with us tonight and here's who you're attacking.

Nicole Perlroth: 55:30 So, they have a much larger degree of plausibility than we do here in the United States. We don't tap the guy at Microsoft or Google or FireEye on the shoulder at night and say, "Tonight, you're hacking the Iranian grid." We just don't do that. But these other nations do. So, how do you agree to a set of norms with actors who have specifically designed their capabilities and their warriors to be outside of the state? It gets much trickier in the fine print.

Demetri Kofinas: 56:01 Yeah. You have all these private militias, essentially.

Nicole Perlroth: 56:03 Yes.

Demetri Kofinas: 56:04 So you said something else, I want to tease it, as we move into the overtime, Nicole, but it's something I want to talk about because one is the ... As we said, this evens the odds. The other is that, increasingly, attacks are being conducted against the private sector and this is another way in which it is substantially different. I mean, the classic attack is the Sony hack by North Korea, which eventually led to the resignation of the CEO because of just some emails that she had written, which weren't incriminating, she didn't do anything criminally wrong, they were just embarrassing.

Nicole Perlroth: 56:34 Right.

Demetri Kofinas: 56:35 I mean, that's the threshold of vulnerability in this particular instance. I want to talk in more detail about the ... Actually, we haven't even touched on it, the recent presumed hack by the Chinese against parts of India's electric grid.

Nicole Perlroth: 56:52 Yeah.

Demetri Kofinas: 56:52 The Indian national electric grid, because that, again, brings us back to some truly ... Again, I'm not trying to be hyperbolic, but some truly horrifying scenarios and real vulnerabilities. I also want to discuss what kind of solutions you think are needed here, because when I had a conversation with Bruce Schneier about this, he pretty much pooh-poohed any ... I mean, he wasn't saying that people shouldn't try to practice, quote, "good cyber security hygiene," but for the most part, his feeling was that this has to come from the public sector because the nature of the problem is such that individuals can't really secure themselves. Now I do wonder, though, to what degree, and maybe this is where you need certain regulations, but should there be clear regulations forbidding certain classes of devices from being connected to the internet?

Nicole Perlroth: 57:40 Yeah.

Demetri Kofinas: 57:41 Yeah. So we'll move that into the overtime. For anyone new to the program, Hidden Forces is listener-supported. We don't accept advertisers or commercial sponsors. The entire show is funded, from top to bottom, by listeners like you. If you want access to the second part of my conversation with Nicole, as well as the transcripts and rundowns to this episode and every other episode we've ever done, head over to hiddenforces.io and check out our episode library or subscribe directly through our Patreon page at patreon.com/hiddenforces. There's also a link in the summary page to this episode with instructions on how to connect the overtime feed to your phone so that you can listen to these extra discussions, just like you listen to the regular podcast. Nicole, stick around, we're going to move the second part of our conversation into the subscriber overtime.

Nicole Perlroth: 58:32 You got it.

Demetri Kofinas: 58:34 Today's episode of Hidden Forces was recorded 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. If you want access to overtime segments, episode transcripts and show rundowns, full of links and detailed information related to each and every episode, check out our premium subscription available through the Hidden Force website or through our Patreon page at patreon.com/hiddenforces. 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.