Tristan Harris: In 2021, there was a cyber attack on the colonial pipeline, the largest pipeline system for refined oil in the US. Carrying 3 million barrels of oil per day, between Texas and New York.

Nicole Perlroth: The United States could have only afforded two to three more days of colonial pipeline being down before it ground the country, our economy to a halt.

Tristan Harris: That's Nicole Perlroth. She spent a decade as the lead cybersecurity reporter at the New York Times.

Nicole Perlroth: It was because colonial pipeline paid this ransom and the criminal group honored their hostage note that they were able to eventually get these operations back up and running, but it is worth pausing to think that all it would take to bring the world's richest economy to its knees is one stolen password. That is what it took. You know, this is what a bumbling cyber criminal group could do. Think of what a nation state could do in this space.

Tristan Harris: As Nicole intimately understands, bumbling cyber criminals and nation states alike can bring entire economies to their knees. Through the mere identification of bugs in our software. So as software eats the world, fragility eats the world. I'm Tristan Harris and I'm Aza Raskin. And this is Your Undivided Attention. The podcast from the Center for Humane Technology, Nicole Perlroth is a member of the Department of Homeland Security's Cybersecurity Advisory Committee. She recently published. This Is How They Tell Me The World Ends. In-depth investigation of the global cyber harms race. Nicole, welcome to the show.

Nicole Perlroth: Thanks so much for having me, Tristan.

Tristan Harris: We are really big fans of your work here, and we have not covered on this podcast, the aspect of cyber defense, cyber offense, cyber weapons. But it actually links very closely. You know, people know us for our work on the social dilemma, social media, which is a way in which to always invoke E. O. Wilson's problem statement that the "Fundamental problem of humanity is we have paleolithic emotions, medieval institutions, and 21st century accelerating godlike technology." I was adding some words there, but the speed of the tech moving faster than our institutions is one of the main overarching issues. And social media is one aspect of that. We've not yet covered on this show, cyber weapons. And just to like frame this up before we get into the whole conversation, we often talk about how, as we look at the world, moving forward, there's these two attractors, it's like a bowling alley.

And on one side of the bowling alley, we have all this new technology that's moving faster and faster and faster. And the cost of that technology is going down and down and down, and into more and more hands. So we have synthetic biology, that's available to more people. We have artificial intelligence that's available to more and more people. We have viral tweets that can be
spreading ideas pneumatically or through information warfare to more and more people in that capacity is being decentralized. So we call that the chaos side of the gutter of the bowling alley. And then in response to that is another gutter called oppression. Which is the, let's lock everything down and make sure no one can do anything with anything. We don't want people to have synthetic gene printers in their basement. We don't want people to have CRISPR. We don't want people to have social media where they can reach millions of people.

So let's create a free speech monitoring top down system that monitors what people say or the China's model of censorship. And so these two attracts these two sides of the bowling alley in framing that up again, we have not yet talked about in this program, the history of the cyber weapons arms race, and that this is really a critical and an important aspect of how the world is going to have to navigate itself if we want to find this third attractor of some digital open society that is able to somehow binder control this decentralized power that's available in more and more hands, but not create these totalitarian societies you don't want to live in. So with that said, we are so excited to have you on, and maybe starting with a story. I know you had this special salmon dinner in Las Vegas, and I think it'd be helpful for maybe listeners to hear, how did you get into this? And, how did that dinner in Las Vegas lead you to do this?

Nicole Perlroth:

So one correction is that it was actually in Miami. Most hacking conferences are in Las Vegas. Black Hat, DEFCON, all in Las Vegas. This conference that you're referring to is a very special subset of the cyber security industry. S4 is the name of the conference. And every year in Miami, they pull together industrial cyber security experts. People who specifically focus on the cyber security of the software that makes its way into pipelines, nuclear plants, hospitals, water treatment facilities, the power grid. And I was invited to this conference and I show up, and the first night the conference organizer, who's a former NSA Codebreaker named Dale Peterson, invited me to dinner. And we go to this dinner in Miami and it's Dale, it's a person named Ralph Langner, who is a German industrial control security specialist. So I was sitting next to Ralph.

And then on the other side of the table were two Italian hackers who had a very interesting business model. And they searched for bugs in the software that makes its way into industrial systems and they sold them to anyone. And so the question on my mind was, who are you selling these to? And maybe more importantly, who will you not sell these to? I really wanted an answer. Because what they were doing was they weren't just selling bugs in Internet Explorer. They were selling bugs that could be used by bad actors to shut down a pipeline, trigger an explosion at a pipeline, shut down the grid, shut down a pacemaker. The possibilities were endless. So I kept asking this question, who do you sell to? And they wouldn't answer. And finally I said, okay, well, who won't you sell to? Iran, North Korea, China. And of the two Luigi had the better English.
And you could tell, he was just sitting there thinking about my question, staring at his plate. And finally he said, "Nicole, I could answer your question, but I'd rather talk about my salmon." And at that moment, Ralph just exploded. Because, here is a guy whose job it is to try to plug basically every one of these bugs and vulnerabilities and protect these critical systems who had seen just how many more systems were still vulnerable. And the Italians were clearly making his job a lot harder. And so he just exploded at the table. And the way I remember it is he said, Nicole, these men are young. They have no idea what they're doing. They have no idea that one day they might have blood on their hands. And then he turned back to Luigi and Donato and said, but tell us, tell us about your fucking salmon.

And from that point on the fucking salmon, just percolated in my head for years and years and years until the point where I said, "I have to write a book just about this market for bugs and where it's going. And just how many players beyond the usual suspects are now buying these bugs." Because the reality is that 20 years ago, there were only a few players that had the people with the knowledge and the skill sets to find these critical bugs and to exploit them in such a way that not only were they powerful tools for intelligence and counterintelligence and espionage, but sabotage and destruction.

And unfortunately, because of this market for bugs, the number of players who can play in that space is endless. Because even if you don't have the people with the skills or the tools, you can now buy them from the Luigis and the Donatos of the world. And what really sucked me in was the question of morals. Who can sell these? Who are they selling them to? Who don't they sell them to? How do they sleep at night? How do they know how they will get used or how they won't get used? I couldn't believe that there was a market out there for these tools, for the raw material, for cyber weapons and spyware, and nobody was willing to talk about it or answer any basic questions. And so that is what led me down this road.

Aza Raskin:

You know, one of the things I have to say, Nicole is, as I've listened to your work, the number of times I've had to pause and absorb what you say. And I realized a big part of the problem is the language that is being used. Like, I've heard you say the word bug, bug bug bug, but to me, what a bug is is like my iPhone glitches out, like on my computer doesn't start as fast. Like the font is a little bit weird. It's not in the same class as a thing that a person can hit a button, one side of the world and create an explosion in a petrochemical plant in another side of the world. That's like a different thing. Same thing with cyber.

It's like, I've been hearing about cyber attacks and ransomware attacks for a while, but it wasn't until I really like hit pause on your podcasts and listen that I realized these aren't actually cyber attacks. It creates explosions in the physical world. And every time we say the word cyber it's obfuscating, the true impact. And so I'm just curious to hear you react to that. Like, is that true? Is that like a
frustration that you have, and then are there other better ways that we could talk about this that elevates its importance so it actually fits the physiological, like folds of our minds?

Nicole Perlroth: Yeah, it's such a good question. So when I got on this beat, everyone hated the term cyber Pearl Harbor. Everyone was warning of a cyber Pearl Harbor, but most of the people in the cyber security industry said, that's fear mongering. You're scaring people to sell your security software. And unfortunately that is a real dynamic, but there is another reality that has become very clear, which is that okay? Maybe we don't use the word cyber Pearl Harbor, maybe that's fraught. Maybe we actually use the word cyber Fukushima, because that's what is happening here. I have seen Russian hackers probe our nuclear plants, and they are not there for intellectual property theft. They are probing these plants for bugs in the software that touches these critical systems, just like Stuxnet did. And it's worth actually just lingering on it for a second.

Tristan Harris: Stuxnet is a cyber weapon that was co-developed by the NSA in Israel around 2006 to infect Natanz, which was Iran's nuclear facility. It exploited bugs in Microsoft and Siemens industrial control software in order to control the speed of nuclear centrifuges. The NSA in Israel somehow got someone carrying a USB drive that had Stuxnet to walk into Natanz and plug in the USB drive, which unleashed the code. If you were an engineer at Natanz, everything looked like it was functioning perfectly, but over a period of months, Stuxnet took out one fifth of Iran's uranium supply and then Stuxnet got out, which is how people realized what the US and in Israel had done. It ended up infecting hundreds of thousands of systems worldwide, including those of American companies like Chevron. It was designed not to damage systems that were not at Natanz, but it still infected them. On the one hand, Stuxnet was an extraordinary counter-proliferation effort involving no physical warfare or bombs or weapons. On the other hand, it showed the world what was possible with bugs and code.

Nicole Perlroth: So since then, over the last 10 years, I actually joined The Times in 2010, the year Stuxnet got out. And what I covered over the next 10 years was the post-Stuxnet era. This era, in which every government on the planet and cyber criminal groups woke up to the potential for code both for espionage and destruction, and started investing in the development of, or acquiring offensive cyber attack tools. And the raw material for those tools is bugs in the code. Bugs and iOS, Apple, iPhone software. Bugs in Schneider Electric's safety locks. The very thing that prevents some kind of explosion at an oil facility or a petrochemical plant. And I started covering attacks where actors like Russia's GRU or others were caught using these bugs. We started seeing nation states conducting attacks using these bugs in the code. And so the cat really was out of the bag.

And that is why it was critical, I think, to call this out that we are now living in the post-Stuxnet era, because most Americans still don't even know what
Stuxnet is. They don't realize the Pandora's box that was opened in 2010. And then to my earlier point about the fact, no one wanted to talk about this. We needed to talk about this because clearly when software is now eating the world as Marc Andreessen says, Well, no one paused to say, is that a good thing? You know, are there some systems that are so critical to our lives, our safety, livelihood, freedom that maybe we shouldn't be baking buggy software into those systems. And that the reason governments like ours were stockpiling, these bugs was justified by national security. We need these bugs because we need to shut down Iran's nuclear enrichment program.

We need these bugs because we need to be able to spy on this Russian official or this Chinese official or terrorists. The problem is that 25 years ago, if the NSA found a bug in Chinese software, Russian software and held onto it, didn't disclose it. There would be no foul, no harm to Americans because we weren't using that software. Today, for the most part, with a few exceptions, we are all using the same software. So when a government like ours holds onto a bug in Apple iOS software, or Siemens industrial software or Schneider electric software, they're not just holding on to it for their own operations. They are necessarily leaving their own people vulnerable. And also increasingly our own critical infrastructure vulnerable as software started making its way into these critical systems.

Tristan Harris: I’d love for you to tell the story of the colonial pipeline, which this is another was a moment where I had to pause your podcast. And I'm like, oh, this was a successful attack against the US that only via the good graces of the people that attacked us, it could have taken the entire us down.

Nicole Perlroth: Yeah. So one of the issues with this space is that it truly is asymmetric. I don’t think people realize the United States is now among the most targeted countries by cyber attacks. And you could argue among the most vulnerable, because we have such a wide complex attack surface. Now that we have plugged software into everything we do. And most of the people who are just putting the software in are not thinking about how it could be abused or used against them. So some of the worst attacks we’ve seen, aren’t even the sophisticated bugs that trade in these underground market, which are called zero days.

Speaker 3: Zero days are bugs in software that the software company doesn't know about. That’s why they’re called zero days because the second they’re exploited against people who use the software, the software company has zero days to fix them. A zero day exploit is therefore a cyber attack that uses zero day bugs.

Nicole Perlroth: So some of the worst attacks we’ve seen, aren’t even the sophisticated bugs that trade in these underground market, which are called zero days. They’re configuration errors. They're somewhat not turning on two factor authentication. And that is the story of colonial pipeline. A bumbling cyber criminal group didn’t even have to develop the code themselves. They actually
rented ransomware code from a criminal group that rents out ransomware as a service. They rented it out and they used it to breach colonial pipeline and hold colonial pipelines, business network hostage. How did they get in? Because colonial pipeline forgot to deactivate an old employee account. That employee had a password, and the company had not enabled multifactor authentication. So all it took for this criminal group to hold colonial pipeline systems hostage was a stolen password.

They didn't actually get into the pipeline. That's important. They got into the IT systems. They didn't get into what's called the OT systems, the operation. But they hijacked their network in such a way that colonial pipeline couldn't get billing information. That their confidence in their operation was so shaken. They weren't sure whether it was possible for these cyber criminals to hold hostage, the pipeline itself. So the company actually took the preemptive step of shutting down the pipeline. And we all saw what happened next on TV, where we saw people panic buying at the pump. We saw people trying to fill up plastic garbage bags with gas. We saw nonstop flights get grounded, but what you didn't see is something I got in my reporting with David Sanger on this attack, which was a confidential department of energy assessment that concluded that as a country, the United States could have only afforded two to three more days of colonial pipeline being down before it ground the country, our economy to a halt.

And it was interesting. It was not so much the oil or the gas. It was the diesel required to run our factories. If you couldn't run our factories and manufacturing, we were in trouble. And it was because colonial pipeline paid this ransom and the criminal group honored their hostage note that they were able to eventually get these operations back up and running. But it is worth pausing to think that all it would take to bring the world's richest economy to its knees is one stolen password. That is what it took. And unfortunately, I would love to tell you that colonial pipeline is the outlier. Unfortunately, they are very indicative of the sad state of America's cyber security and cyber defenses. That is how unprepared we are. You know, this is what a bumbling cyber criminal group could do. Think of what a nation state could do in this space.

Think of what if a nation state decided not to bring the operation back up and running, or they didn't just hit one colonial pipeline, but five colonial pipelines. Then you start getting into a new realm where these are also powerful psychological tools. You know, right now, we are all complaining about the spike and gas prices, and it is looking like it will have a huge effect on the upcoming midterm elections. This is what people care about most apparently in America.

Think about a coordinated Russian attack on the equivalent of five colonial pipelines, which is entirely possible and what that would do to influence an election or to influence Western support for the sanctions that we are putting in place against Russia for their invasion in Ukraine. And you start to see that it's not necessarily that Pearl Harbor, the explosions that are the most likely
scenario, or would even be the most effective. It would be these coordinated stealthy attacks on our pipeline systems that would shut them down and become a huge psychological political tool. Those are the ones I really worry about, or a leak at a nuclear plant where it's not entirely clear who started it. It would take time to pinpoint how it began and who was behind it. And you start to see just how much more pernicious a cyber attack could be than some of the traditional attacks that we talk about in the realm of Pearl Harbor, 9/11.

Tristan Harris:

There's just so much to impact with everything you're sharing. One is the stakes and to Aza's point about language, I think when we call it a cyber attack or a bug in code, what if we called it a hospital attack, a chemical plant attack, a water system attack, a nuclear power plant attack, an oil pipeline attack, an air traffic control system attack. You started to get a different picture of what these things are when we don't talk about them as bugs and code, but in terms of the systems that they're affecting. And to your point, we are rapidly wanting to digitize just about every single vein in our central nervous system of our economy. And part of that, actually, it's interesting. It's also linked to economic risks, right? Because actually economic growth, we make a lot more money when we can sell people's stuff.

That's like the digital version of the thing they have. So why don't you want the digital lights for your house? The digital heating system, the digital energy system and economic growth comes with that. But basically as we are digitizing our society, to the point of Marc Andreessen's software, eating the world, we are making our society fragile. So when software eats the world, fragility eats the world. And so the trend of market incentives driving a mass digitization, which basically going from analog slightly more secure infrastructure to a mass attack surface area that is digitized where they're not incentives, because the company that tries to make sure that security is embedded in their thing. If they get outcompeted by another company that's going faster and has race to market dominance. So the company that gets there first is often the one that wins. And so the way to get there first is to not do it with all the security stuff baked in unless you're incentivized to do so.

So we end up in this growing attack surface area combined with a lower and lower cost to actually hack that surface area and then a kind of oblivious public, because this is not legible in the simple way to everyone. And so just framing some of that up, it just makes you pause and think about which world we're really living in. And this again, gets back to paleolithic emotions, medieval institutions, because where is the regulation and the protection. And is that even possible when the speed of the technology means that generally speaking, the way to keep winning is to just move faster and faster in the arms race, which basically means moving faster and faster into danger. I'd love to also name what the stakes of this are. You're talking about the colonial pipeline and Hey, we're only two days away from basically being brought to our knees. Give us a taste of
what happened maybe in Ukraine. So there's a little bit more of an experiential sense for listeners maybe.

Nicole Perlroth: Yeah. And just as you were talking, I was thinking it’s not just software eats world, not to pin everything on Marc Andreesen and Mark Zuckerberg, the Marks, but it's been a collision over the last 10 years of move fast and break things and software eats world. There were no incentives to say slow down, make sure your code is secure, check your mistakes, because your code is going to be used in systems that would allow for massive breaches of people's personal data and increasingly an act of sabotage on our critical infrastructure. No one was talking about that threat model. So for years, Ukraine really has been Russia's test kitchen for a lot of different attacks. They've had fishing attacks, they've had attacks on their media organizations. They've been a testing ground for disinformation campaigns and propaganda. The attack that I don’t think people discuss enough was an attack in 2017 called NotPetya. Sometime between 2016 and 2017, someone appeared on Twitter and they claimed to have hacked the NSA, and to have stolen the NSA zero days, these bugs.

And over the course of several months, they started dribbling out these bugs, information about what the NSA had, some of their most coveted, offensive cyber tools. And within weeks of that release, there was a gigantic ransomware attack by North Korea, that hijacked systems all over the world. A month later, we saw Russia use that same stolen NSA zero day exploit in what initially appeared to be a ransomware attack on Ukrainian government agencies, but was not a ransomware attack. Because even if you paid, there was no way to get your data back. And that attack didn’t just hit Ukrainian government ministries. It hit the railway systems. It got into the radiation monitors at the old Chernobyl nuclear site. And it didn’t just hit Ukraine. It hit any company that had even a single employee working remotely in Ukraine. So it hit Merck. The untold story actually of that attack is what happened to Merck.

Merck had an existential crisis. They had to tap into the CDCs emergency supplies of the Gardasil vaccine that year, because their vaccine production lines were completely paralyzed in that attack. I think with the escalation of Russia's invasion into Ukraine, with the support that the West has given Ukraine, at some point Putin will respond. And I think the most likely avenue for some retaliation is a cyber attack. Similar to what happened with NotPetya. It was interesting when NotPetya happened, I went to Ukraine because again, this is the test kitchen and what the Ukrainian said to me after I spent weeks going through the innards of these attacks and understanding what the true impact was, was this. They said, listen, "We think we are the test kitchen. And we think you are the end target. And the difference is that when this attack comes your way, it will be so much worse. Because for the most part, we're still pretty manual and analog here."
You know, we still do our elections on pen and paper. We are not putting Schneider Electric software into every part of our critical infrastructure. And in fact, these attacks have been such a wake up call that it’s an opportunity for us to rebuild a lot of our economy from scratch and think very carefully about which systems are so sacred, we don't want software touching them at all. But you are fully automated and you are only rushing into the age of automation and machine learning. And so when it does hit you, it will be that much worse.

And that really was the message I thought, wow, we need to take this home. And people need to understand that there is this confluence of dynamics of software eats world, of move fast and break things. And the last thing I'll say on this is just our adversaries know that they might not ever be able to match the Pentagon's budget in terms of military spending. But they now know we have a very soft underbelly when it comes to cyber and they can do a lot more harm with these methods perhaps than they could even do with kinetic weaponry.

Aza Raskin:

I think many of our listeners are of course familiar with the internet of things and to understand that like the cameras they put in their home and the thermostats and they put in their home are pretty vulnerable and that hackers can like get in and listen to their conversations. That's when I think, before listening to you, when I think of like cybersecurity, that's where my mind goes. And the realization I had especially as you speak now, is that we're not talking about the internet of things. We're talking about the internet of national backbones. We're talking about the internet of our life support systems as nations and as cities. And when we've been looking into of more our domain, like social media, one of the things that we constantly see is that we used to have protections in the physical world that get lost when we move to the digital world.

We used to have regulations around what kids could watch on morning cartoons, but when you move to YouTube, all those protections just go away. And I'm imagining the US military saying like, you know what, yeah, we're in on the Navy, we should definitely have Navy and we're in on the army. Yeah. That seems like a good idea, but you know what? We just don't need an air force. We don't need one of those things. And that's the place we are now with our fundamental infrastructure is that the US is saying, I guess we don't need it. So that's the question I have for you. It's like, I think in one of your interviews, you pointed out that 80% of the critical infrastructure of the US is now run and operated by private companies. So, obviously we must have laws that make these companies beholden to the country that gave them birth, right? Like there must be national security laws that say you guys have the responsibilities and obligations so you can step out of like the competition that Tristan was talking about before. So do we have those laws?

Nicole Perlroth:

No. And you know, I always think in the physical world, how I was pulled over recently, because the sticker on my license plate was out of date. And yet there's
not even a body who would come in and investigate whether a company like Colonial Pipeline has multifactor authentication, enabled. There's just nothing like it. There was an attempt in 2012 to pass a cyber security bill that would've mandated strict cyber hygiene standards for the companies that run America's critical infrastructure. Chemical factories, nuclear plants, power grids, pipelines, water treatment facilities, hospitals, telecom networks. It failed because lobbyists from the US Chamber of Commerce successfully convinced John McCain, the late Senator from Arizona, that those cyber hygiene standards would be too onerous or too expensive for business. And I don't think that Senator McCain truly understood cyber security or was very technical or took the time to understand what the threat actually was.

And so he filibustered and we never saw that bill passed. And over the last 10 years, any cybersecurity regulation we've had has come in the form of a toothless presidential executive order. We saw them from Trump. Most recently, we saw them from Biden. Now what Biden did with the most recent cybersecurity bill he does deserve credit for because it's the most comprehensive we've seen. And it really clearly understood what the government's limitations are in this market. So what they had to do is say, okay, we're handcuffed here, right? We have no authority in this space. There's no laws in this space. This is an executive order. Who do we have control over? Well, we have control over federal agencies. So we're just going to mandate from now on that federal agencies meet these strict cyber hygiene standards. And we don't really have control over private business, but we do have the power of the purse.

And we can use that to say that any federal contractor needs to meet these standards. Otherwise, we won't do business with them. So what they did was they said, listen, we'll rip out the red tape. You don't have to get some third party auditor. We'll even let you self certify that you meet the following cyber hygiene standards. But if we catch you lying to us, which we will, because likely you'll get hit by a ransomware attack that exposes the fact you didn't patch your systems. You are banned from ever doing business with the federal government again. So, that's the first stick we've seen in this space. Now, very recently, just in the last couple months, we did see a breach disclosure law passed that mandates that those companies that run 80% of America's critical infrastructure have to disclose when they've been breached. And that is a good thing. That's nothing to sneeze at.

Because when you see these attacks happen on one company, there is a very high likelihood that they were not the only target. Usually, particularly, with cyber espionage from China, we see state backed hackers go for an entire industry. So, that is one step forward. But there's still a long way to go. And really the federal government is left in this position to essentially beg the private sector to disclose these breaches, to raise the level of cyber hygiene. And again, when all it takes to hold the biggest conduit for gas and oil and diesel to the
Eastern seaboard is a lack of multifactor authentication and a poor password. It's hopeless. And that is where government has a role to play.

Tristan Harris:

And part of the medieval institution bit is that medieval laws, right? So our laws are moving always slower than the way that the tech might change, even the definition or the meaning of the moral concepts that we used to hold dear. And so the way that we define the boundaries on our laws is also being outmatched by the speed and the unique characteristics of the tech. And I think, again, we come back to that E. O. Wilson quote. It seems like if we zoom out, there's just this overall effect of the things you're talking about, which is a fundamental change in the symmetries and asymmetries of power.

In the medieval times, if you have a castle, that was a new defensive technology. So now cannons broke past some of those defenses, but then what the cannon was to the castle, I would say social media is to the nation state and cyber is to the nation state. Because, no matter the fact that you've got those patriot missile defense systems or those F35s, the chinks in the armor, as you digitize your society, the "entire armor," that we're wrapping around our society with a digital actually basically puts us in a vulnerability suit.

We're wrapping ourselves in a vulnerability suit. Because while we have an air force and a Navy and a space force, we don't have a metaverse force or an Instagram force. We do have a cyber defense force. But as you said, the issue is the public-private nature of the relationship when 80% of our infrastructure is created by private companies and the government has limited abilities to mandate things. I love your idea though, about just like you got pulled over, because you didn't, you had an outdated smog check. Like why don't companies all get pulled over for having an outdated security check? I think these kinds of metaphors go a long way in just making it clear for us that there's a collective action problem. And if I do it and the other guy doesn't, then I just added a bunch of cost to my balance sheet. And meanwhile, the other guys are getting off free. And so unless there's enforcement for everybody, it doesn't make economic sense.

Nicole Perlroth:

Yeah. And we need metrics. I mean, we all have FICO scores. What is the risk a credit card company is taking on when they give us a credit card, we don't have that in cyber. We don't have the equivalent of a FICO score for the supply chain. So when you take on a vendor or you acquire a company or you adopt Open-source code, you have no idea how much risk you are taking on by working with that company or that code. So there are companies out there that are working on creating ratings security ratings, just from what they can gather outside the organization. They'll look at your organization and do a scan. Say, do they have a server? That's just sitting out there on the open internet or it's unpatched. We will lower their score. But we definitely need metrics.
The other thing is when you go back to your bowling alley analogy between chaos and oppression, and we talk about software eating the world, move fast and break things, where the incentives lie, which are only leading us towards further vulnerability, this market that has crept up that incentivizes hackers to just sell their bugs under the table to governments for millions of dollars, not see to it, that they get patched.

You really get a sense for chaos, for the potential for chaos. On the other side, on the oppression side, what China did over the last two years is they put in place new laws to try to control this chaos. And the laws say, if you are a Chinese hacker security researcher, you are forbidden from attending Western hacking conferences and presenting all the ways you can break into a Tesla or an iPhone or Schneider Electric. You can't do that anymore. That's illegal. Also, if you find a zero day, which is a bug in code that the manufacturer doesn't know about, you have to give the state right of first refusal on that bug. So basically they are cutting the market out at its knees. The other thing is that the US and the west no longer dominate the market for these goods. If I'm a hacker and I find a zero day bug in your iPhone software, your iOS software that can remotely read your text messages, track your location, do all the things I would need to do to slap an invisible ankle bracelet on you.

The going rate for that iOS zero day exploit, I just described, I believe is $2.5 million. If you sell it to a broker in the United States. A Saudi Emirati dealer called Crowdfence. Last time I checked their pricing, it was $3.5 million. So we're already getting out-priced by a million dollars. And all of these hackers, they're not sitting inside the United States. And for my book, I went down to Argentina and I met with people there. And I had a very interesting conversation with old hacker there who's not in this market, but he's the godfather of the hacking scene and Argentina, for a number of factors, cultural education are very good at finding zero days and exploiting them and they can make a good penny and skirt inflation by selling these two brokers all over the world. And I asked him the same question that I asked Luigi and Donato so many years earlier.

I said, well, who will they sell them to? And I regret how I phrase this, I apologize to everyone in advance, but I said, "Well, you only sell these to good Western governments." And he laughed in my face. And he said, "Nicole, the last time I checked the country that bombed another country into oblivion, wasn't China or Iran. So we don't share your moral calculus." Most people will just sell these to the country that hands them, the biggest bag of cash. And right now that biggest bag of cash isn't a US broker, it's an Emirati broker or a Saudi broker. And how are they using zero days? Largely to try to preempt what they see as their biggest national security threat, which is another Arab spring. So for the most part, they are using these for spyware and surveillance tools on their own people on dissidents and journalists and human rights activists.
Tristan Harris: To put that 2.5 million into context, right? Certainly the US has more F35s than anyone else in the world. For the cost of an F35. You could buy 2000 of those exploits per day for a year. And so it just shows you this shift in a symmetry. The image that I have in my head is like on our move to digital it’s we have this double whammy, because we’ve built a brain implant into the brain of society, and that’s both social media and it’s also our infrastructure. And we’ve left the electrodes of that brain implant, just sticking out for anyone to touch, whether it’s like bumbling criminals or whether it’s nation states, and you can touch some of those electrodes and you can stop all the gas flow or the diesel in the US and bring our nation to its knees.

Or you could find a zero day exploit in the psychology of the US, which is finding those culture war like fault lines and using Amplifi Ganda to heighten those tensions. And so now we’re getting hit doubly, both at our infrastructure level and at our cultural level. And that’s the connection between our work and yours totally. And just to even pair it back to something that you said. How the Twitter trending topics list is basically the zero day vulnerabilities for the cultural fault lines of democracies. Because you basically, we’re we’re publishing, Hey, here’s exactly where to hack us and cause division and chaos. Just talk about any one of these 10 topics that are trending and I guarantee you’ll get visibility, engagement and division. So just amplify those. So we’ve walked deep down into this dark valley. It feels pretty hopeless down in here. What are the kinds of ladders that you can show us where we can start to see how it might climb up?

Nicole Perlroth: So, okay. Couple ones. One is, and this is the most frequent question I get asked right now, is why haven't we seen more cyber attacks from Russia in Ukraine or in the West as a result of Western support for Ukraine? And I think that is a great question. And I think we are watching the potential limits of cyber attacks and cyber war play out in real time. Now I should back up and say that there have been a number of very serious cyber attacks against Ukraine from Russia. We saw them hack ViaSat, which was an attack intended to basically disrupt everyone's connection to the internet. But I guess thanks to Starlink people have still been able to connect and broadcast every video in these images from the invasion. So that didn't go as well as planned. They also did hack several Ukrainian power stations in the days, going into the war and Ukraine, cyber defense with some help from, I believe the United States and Western allies, they were able to discover that attack before it detonated.

So that is one point of optimism. Even without these laws, even with this disconnect between the private sector who run our critical infrastructure and the federal government, I have to say that one area for optimism is that no one is letting the Ukrainian crisis go to waste. I have never seen the level of real time collaboration between the federal government, our allies and the private sector and the cyber security industry that I am seeing right this minute. There are slack channels lighting up where everyone is voluntarily disclosing anomalous behavior, malware strains that they’re catching on their network and companies,
particularly well resourced companies are really able to do what the federal government calls shields up. Basically act like you're about to get breach or soon breach. Now that raises other questions about what some call cyber security poverty line, which is, okay, that's fine for the Johnson and Johnson's of the world and the Fortune 500.

But when so much of our critical infrastructure is run by mom and pops who are running the local water treatment facility and don't even have a single IT guy in the building and are running Microsoft windows software that hasn't been patched in years. What about those guys? Because the impact from an attack on them, is in some cases, arguably worse than an attack on a Merck or Johnson and Johnson. So we have to deal with that. But for right now, we have come a long way in a very short amount of time. And I am hoping that that will continue. Another ray of hope is there was a study done back in, I believe 2016. So it's out of date. And if anyone wants to pick this up, who's listening, please do. But using semantics data, a group of academics and researchers looked at attempts to breach a country systems versus successful attempts.

And they looked at okay, where are the countries in the world who they're seeing their fair share of cyber security incidents or probing, but they aren't actually getting breached. Who are those countries? The answer was in Scandinavia, Finland, Sweden, Norway, Denmark actually do a pretty good job of deflecting a lot of the cyber attacks and incidents that come their way. And so the researchers looked at okay, why are these countries somehow better prepared than everyone else at cyber defense? And the answer is that they have national comprehensive cyber security policies in place that they update every year, along with the threat that have real carrots and real sticks for companies that operate the country's critical infrastructure. They get fined if they're not using multifactor authentication, they get fined. If they, they haven't upgraded their software to the latest patched version of windows or iOS or Schneider Electric or whatever it is.

So what that tells you is that we need a comprehensive national cyber security policy with laws that have real teeth, that are finding people when they don't do the equivalent of getting smog check. You know, that is just not one of those things where regulation makes it all worse. It is an area where we have neglected our responsibility to national security by not mandating that these companies meet strict cyber hygiene standards and finding them when they don't meet those standards. We don't have that here. Regulation has become such a dirty word that no politician has been willing to re-up this fight. I mean, we finally have leadership in place that I think is regardless of how you feel about the Biden administration. There's no doubt that they have done more over the last year for cyber security than any other administration on record, but it's not enough. You know, we still have so far to go.
Tristan Harris: What worries me, and I have friends who work in cyber security, who were saying at the beginning of that Ukraine, Russia war. That what happens when all of those cyber hackers who are perfectly happy before to accept a couple million dollar payout are now not motivated by money, but are motivated by geopolitical ambitions. And it's like Brazilian jujitsu. I put you in the posture and I am locking you in and you can't tap out. Before you could pay me and I'll release my grip. And now I'm not going to release my grip because I simply have that motive. And I think that's one of the things I'm increasingly worried about as we go on. There's another story from the Ukraine war when Putin went in, it activated, obviously everybody who disagreed with that decision, the entire global hacking community. He didn't just declare the special military operation or war against Ukraine. Everyone in the world who was a hacker who was against that could now, as non-state actors, just say, you know what, I'm going to go after hacking the GRU.

And so what's also difficult about this environment is the lack of attribution. Because now you have 17 year olds in their basement in Argentina who are saying I don't like Putin either. And so they're collaborating with hackers in the Netherlands and in Norway and random places all throughout the world. And they're making changes to directly wipe software and files from the GRU's computers. There's a specific example of someone who was running a famous JavaScript library and they updated it to basically say, if this library that I wrote is being run. If this code is being run inside of Russia, then basically wiped the computer that I'm on. And this code library was shipped. You know, they did a little software update and then everybody who was running that code library in Russia, their computers were wiped. Now what happens when Putin thinks that was actually the US or the CIA and not some independent 17 year old sitting in his basement in Argentina?

And so the decentralized nature of a war of all against all, this hobbys in a sense creates again, more of that attract towards this chaos. And so what I hope though is that we're moving to this period of such net fragility across the board that we recognize how unstable the situation is and that we have to be very careful about assuming that there's an action taken. But the problem of course, is that many more of these decentralized actors can trigger something and make you believe that it was actually a US hacker, because they could have also disguise themselves. So it gets infinitely complex.

Nicole Perlroth: And I share the concern. I mean there was so much rah rah around what groups like Anonymous we’re doing in the beginning of the Russian invasion by infiltrating Russian state television outlets and broadcasting actual images of the Russian invasion. And I shared that enthusiasm until I thought about a couple things, which is one, the potential for escalation and two, the fact that Putin, because I do believe this is one man's war, that he is a conspiracy minded fellow.
He thinks that Hillary Clinton and the CIA were behind Ukrainians getting together in independent square and kicking out his puppet government. So it’s a real consideration to think that he’s not going to look at what Anonymous is doing as some individuals gathering around the globe for one cause, but as a hidden Western intelligence operation that he would respond to accordingly. And then to your point, Tristan, about perhaps things like the Russian invasion or Hey, maybe the overturning of Roe V Wade in the United States, maybe people are starting to say, I don’t want to get this fixed so that this government can be more secure. Or I’d rather sell this to someone who can hack that country or those systems.

I think that is a very real consideration. And I am actually shocked we haven’t seen climate activists participate in this market and try and hijack coal companies or major contributors to the climate crisis using these methods. But I think at some point that’s coming. And then finally, to your point on attribution, this is a real issue. You know, attribution has gotten way better now than it was 10 years ago. Western governments, at least, have been much more quick to attribute some of these attacks. Now there’s this question of whether the public will believe them. Which is what happened with Sony when they did attribute it to North Korea, there was this period where no one wanted to believe that intelligence. Likewise, when the Biden administration came out and said, Russia will invade Ukraine on this week, there were a lot of people who said, you’re a liar.

Attribution is very difficult and we’ve actually seen some of these nation state actors actively playing around with attribution. So for instance, a couple years ago there was an attack on a French television network that took out several French television stations and put up pro ISIS propaganda. So everyone assumed, okay, this is ISIS. It took several months for them to actually attribute that attack back to Russia’s GRU. There was an attack on the South Korean Olympics, the opening ceremonies where no one could get into the opening ceremonies because the ticketing system had been hijacked. And everyone assumed, oh, this has to be North Korea, but it took several months and they found out, oh, this was the GRU. And then there was an attack on a Saudi petrochemical facility, where someone broke in and they neutralized the safety locks. Now in the process, they had a bug in their code that shut the whole plant down.

And everyone assumed initially this had to have been Iran because Iranian hackers had been hacking Saudi oil facilities over the past few years. And so it took a long time before researchers said, actually we were able to tie this back to a secret arm of the Kremlin. So why is Russia hacking French television networks pretending to be ISIS, hacking the South Korean Olympics, hacking a Saudi geek petrochemical facility? Why are they doing these things? Well, I think the answer's pretty simple. I think they're playing around with attribution. They're experimenting to see what could we get away with that won’t
immediately be pinned back on us? Because we know that they have the
capabilities to cause a cyber attack that would cause serious destruction. Like
the power grid outages in Ukraine. We know that they have access in too many
cases already to our infrastructure, to critical infrastructure around the world
that we've seen them probing for years.

But what they haven't done until now is pulled the trigger on the access and the
capabilities. And I suspect that is because we have stumbled into a new era of
mutually assured digital destruction. Where yes, they might be in our systems.
Yes. We recently declassified a report that said that Chinese have been probing
our pipelines to get a foothold in the event of some escalating geopolitical
conflict. But I've also reported that cyber command has hacked the Russian grid.
So we're all in each other's systems. And so no one actually wants to pull the
trigger because they know that the minute they do that their adversary could do
the same back to them. So we do have a little bit of this very messy, mutually
assured digital destruction. And I think that's why attribution becomes critical.

Aza Raskin: Tristan, your analogy of everyone, having everyone else in a jujitsu headlock.
And because everyone is head locking everyone else, we don't do anything. I
think when I think about what your work points at as an even more fundamental
trend is that we're moving from mad, Mutually Assured Destruction to all MAD,
where it's not just nation states that can do this to other. Nation states, but can
be an individual who now buys for $2.6 million, one of these zero day exploits
and launch it as a nation state. And how do you do attribution to that? And that
problem of decentralized James Bond weapons for everyone, where we get to
retain some version of our liberties is the central problem of our times. And your
work is highlighting the ground zero of that. So thank you very much for coming
on Your Undivided Attention.

Nicole Perlroth: Thanks everyone.

Tristan Harris: Nicole Perlroth spent a decade as the lead cybersecurity reporter at the New
York Times investigating cyber attacks from Russian hacks of nuclear plants to
North Korea's attack against Sony Pictures. She recently published the New York
Times bestseller. This Is How They Tell Me The World Ends a detailed
investigation of the global cyber arms race. Today, Nicole is a member of the
Department of Homeland Security's Cybersecurity Advisory Committee, and a
guest lecturer at the Stanford Graduate School of Business.

Your Undivided Attention is produced by the Center for Humane Technology, a
nonprofit organization, working to catalyze a humane future. Our executive
producer is Stephanie Lebb. Our senior producer is Julia Scott. Mixing on this
episode by Jeff Sudekin, original music and sound design by Ryan and Hayes
Holiday and a special thanks to the whole Center for Humane Technology team
for making this podcast possible. You can find show notes, transcripts, and much
more at humanetech.com. A very special thanks to our generous lead
supporters, including the Omidyar Network, Craig Newmark Philanthropies, and the Evolve Foundation, among many others. And if you made it all the way here, let me just give one more thank you to you for giving us your undivided attention.