KRISTEN EICHENSEHR: Good afternoon, and welcome. I'm delighted to have you here today for our event on Cybersecurity Beyond the Headlines. I'm Kristen Eichensehr, I'm a professor at the University of Virginia School of Law, and the director of the National Security Law Center.

The National security Law Center is co-sponsoring this event with two fantastic student organizations, the National Security Law Forum, and Law Innovation Security and Technology. I want to thank Peter from our UVA IT team, and our event's director, Rebecca [INAUDIBLE], for their help in making the event run smoothly.

I'm delighted today to welcome Nicole Perlroth. She spent a decade as the lead cybersecurity digital espionage and sabotage reporter for the New York Times. Her investigation and ensuing outing of hacking divisions within China's People's Liberation Army help to compel the first US hacking charges against members of the Chinese military. And it earned her the Best In Business award from the Society of American business editors and writers.

Her articles on the use of commercial spyware in Mexico have been nominated for the Pulitzer Prize, and she's also a bestselling author. Her book published last year, *This Is How They Tell Me the World Ends,* focuses on the Global Cyber arms race. And it recently won the 2021 McKinsey and Financial Times business book of the Year Award.

Nicole is a regular lecturer at the Stanford Graduate School of Business, and was selected as the inaugural journalist in Residence for the University of Texas' Strauss Center Journalism and World Affairs Program. I'm going to ask Nicole some questions to kick off the discussion, and then hopefully we'll have some time for questions and answers.

Please do note that the event is being recorded. And if you'd like to ask a question, please type your question into the Q&A box. So Nicole, let's start off with ransomware, which has been one of the cybersecurity issues garnering a lot of headlines in the United States in the last year.

Particularly last summer, every month it seemed for a while the United States was getting hit with a pretty significant ransomware attack. Can you talk a little bit about the United States response to those incidents and to ransomware more generally. Does the lack of high profile ransomware incidents over the fall and now into the winter suggest that the US efforts to counter ransomware are working?

NICOLE PERLROTH: Great questions. And thank you so much for joining us today, and thank you so much for having me. I realize that we're all doing our 1,000th Zoom webinar, so I appreciate you joining us.

So on ransomware-- obviously it's been top of mind because the ransomware attacks are just getting-- been getting worse, and worse, and worse. And I think part of that is cryptocurrency has been a big enabler. When I first started covering ransomware attacks six years ago, they would hijack your personal PC for $200. Telling you to go to the local pharmacy and give them the pin to some gift card.

Now it's $50 million in ransom demands. And, oh, we're not just going to hold your data hostage, we're actually going to leak it out online if you don't pay us. And in too many cases, unfortunately, victims are still paying because even at a $50 million ransom mark, the cost to remediate from those attacks is still often more expensive than the ransom demand itself.

And the other big enabler for ransomware attacks has been insurance. And I don't think people realize this, but in a lot of cases, cyber insurance underwriters would calculate that it would be cheaper for them to cover the cost of those ransom payments than cover the cost of the remediation. And I think as a private citizen your knee jerk reaction is, well, can't we make it illegal to pay ransoms?

And the case I always point to is a case in 2019, I think, of Baltimore. Which was held hostage for $76,000. Held their ground, didn't pay. Even as their water facilities were being held hostage, you couldn't pay water bills, you couldn't pay your mortgages. The public health systems were frozen. It was getting really bad but they held their ground.

And ultimately, the cost for Baltimore to remediate from that attack was $18 million. That's $18 million that could have gone to public schools, roads, infrastructure. And so it's not necessarily a black or white issue. And the FBI's guidance on this has been, we don't recommend that you pay because when you pay you're just funneling more money into these ransomware groups R&D.

So that's been the story of how ransomware has grown to the point it is today. Now, last year was a banner year for ransomware attacks. You mentioned Colonial Pipeline. There was also the attack on JBS, which is one of the world's biggest meat suppliers.

Everyone probably remembers the price of their Carne Asada going up on menus. There was attacks on the Martha's Vineyard ferry system, NBA basketball, minor League Baseball, on, and on, and on. And the ones that really stuck in my memory were the attacks on hospitals. That were just crippling hospitals and making it really hard for cancer patients to get their chemo because the records of who gets what are fairly complicated. And with no access to those records it was really hard for hospitals to treat cancer patients with chemotherapy.

So stepping back to answer your question, what is this, and has it gotten better since we haven't heard about so many high profile attacks? Ransomware is sort of this inevitable, unfortunately, inevitable evolution of criminal activity.

It's being done by a lot of groups who earlier on in the previous decade had spent most of their energy on spam. And as spam filters got better, they started moving towards ransomware. And at first it was sort of the $200 one-off scams. But then they realized just how vulnerable some of the world's largest companies, and institutions, and critical infrastructure were. And that there was a lot of urgency around pain in those cases because people were so desperate to get their data back. Data has become the new oil.

And so they've really seized on this critical opportunity. And this administration has been trying to tackle ransomware more aggressively than any previous administration. They set up a ransomware task force at the Justice Department. Biden made it his first priority at his first meeting with Putin in Geneva, where he said to Putin, how would you feel if one of your pipelines was held hostage?

And a lot of people wrote that off as Biden being folksy, but I actually saw it as a pretty clear threat. That if you enable what just happened to Colonial Pipeline, better watch out for your pipelines. And what's been interesting is that on the dark web we see this chatter among ransomware cyber criminals debating whether a target counts as American critical infrastructure or not.

There was a ransomware attack a few months after Colonial Pipeline on an Iowa food co-op. And in the chats these ransomware cyber criminals were saying, this doesn't count as critical infrastructure. So clearly it's filtering down into their decision making and their thinking. But it hasn't slowed down ransomware.

I think they've done a good job of just staying under the threshold of the Colonial Pipeline's. Ransomware attacks have continued. And kind of more disturbing is that it has evolved into ransomware as a service. So they basically say, here's the tools, just click on this button and give us a cut of your earnings.

We'll give you the code. And we'll let you use our negotiation platform, and our leak site if someone doesn't pay you. And so the barrier to entry for these attacks has gotten to be so low.

And so we've started to see indictments in arrests, which is a really good thing. In places I never expected to encounter ransomware cyber criminals like Canada, and Kuwait. There was recently an arrest in Romania. Romania has long been headquarters for digital fraud. But it's clear that this is migrating to other places.

We also see nation-states like North Korea leveraging ransomware. And more recently, surprisingly, China. Some of the same hackers who are tapped for nation-state operations were indicted by the Justice Department late last year, and accused of participating in ransomware attacks in their spare time.

So this is going to continue to be a really big problem. Now, the last thing I'll say, because I can talk all day about ransomware, and I'll stop, is in some ways, from my perspective, with all of the attacks I've covered over the last decade, and this really quiet Chinese cyber espionage, industrial espionage. This sort of quiet Russian probing of our critical infrastructure, of our nuclear plants, of our pipelines, of our energy companies have been very stealthy.

It's been easy for victims and targets to just pretend like it didn't happen. Because they have huge incentives to bury those incidents, both for shareholders, and lawsuits, et cetera, et cetera. Ransomware makes it really hard to bury these attacks because they freeze up your network, and that's hard to hide from everyone. And now that they're leaking out victims data, it becomes nearly impossible to bury these ransomware attacks.

So suddenly, all of these boards of directors are saying how do we make sure that we're preventing ransomware attacks? Are we using two factor authentication? Are we logging what's on our network? Are we picking up anomalous activity? Are we investigating it quickly enough? Are we using strong password protocols? Are we educating our employees on phishing attacks and what not to click on?

And all of those things have the added benefit of hardening the nation's soft underbelly that we've had for the last decade, for the attacks I really worry about, which are these more coordinated nation-state attacks. And so in some ways I think I make people shiver a little bit when I say this, but I think it's been a little bit of a blessing in disguise.

KRISTEN EICHENSEHR: That's the most optimistic silver lining to ransomware I've heard. That's a really interesting take. Let me just ask you a follow up question on ransomware before we get into some of the zero-day market issues. So there have been a number of disclosure requirements being discussed in Congress.

Some of them relate to just cybersecurity incidents in general, but ransomware has also furthered that discussion too. And there's been discussion about whether Congress should mandate at least disclosure of ransomware payments within 24 hours, incidence within 72. It seems like that would be an obvious way to help along government awareness, other industry awareness. Why do you think it's been so hard to get some thing like that through Congress so far?

NICOLE PERLROTH: Well, I think data breach notifications are the lowest hanging fruit to improve our cybersecurity. I mean, when you think about SolarWinds, which was this supply chain software attack in late 2020. SolarWinds is used by most federal agencies. And more than 400 of the Fortune 500 Russian hackers, the SVR used their software as a Trojan horse to break into its customer systems.

But as long as that attack did not touch PII, Personally Identifiable Information like your driver's license number, tied to your Social Security number and name, there's no legal obligation for victims to disclose that attack. And yet it almost held our nation hostage. In some ways it still is because there's no clear sense of whether we've even hit the SVR out of those systems however many months later.

That is so backwards. I mean, how do you respond to a threat that no one's even telling you about? It's not as if our government has insight into those corporate systems and vulnerabilities because our laws prevent organizations like the NSA from looking at domestic traffic.

So you could not design a more blind and vulnerable system if you tried. And when you just look at the incentives-- like I was just saying, no one wants to disclose that they've been breached. And so I think this is an area where we do need laws.

I think it's critical to say to these companies, and to provide liability protection to say if you disclose that you were hit, whether it was ransomware, or IP theft, we will give you liability against class action lawsuits. Because ultimately that's the big fear among these companies in general counsels when it comes to deciding whether to disclose the breach.

But it is the right thing to do from a national security perspective. So to me, it's all about honing in on the fine print, and making sure that these companies feel like they're not just raising their hand for a thousand class action lawsuits.

Now, I think we actually got there in this latest proposal for breach notifications. And for whatever reason, it was Senator Rick Scott from Florida who said no. We are not going to pass this. And to be honest, I just felt like that was a huge gut punch because if we can't even get that low hanging fruit passed, if we can't even just force companies to tell us that there is a problem because often they're not the only ones that were hit.

Most times there are-- what would you call it, like a leapfrog into the next victim. How are we ever going to deal with this? And so I think we have a long way to go on educating policymakers. And to me that's been the biggest vulnerability that's getting exploited in this space. That lobbyists are able to step in and convince lawmakers that we shouldn't have these laws.

And I think those policy makers are guilty of really not understanding the depth of the threat, and the situation. And just how dire it has become. So I'm hoping there will be progress on that front.

I was happy to see in the SolarWinds case that, Mandiant, which was the first to raise their hand on this, came out and did the right thing and told the NSA, and told the press, we've been breached. We think they stole our red team tools. We don't how far this goes but we think it's Russia, and we think it's really bad.

And then a month or a few weeks later they said, OK, we've been investigating, and we see it came in from SolarWinds, which is an American company software. And so everyone needs to check if you're using SolarWinds software, that you don't have the SVR on your network. And they had no legal obligation to do that.

But think about where we would be if they'd never told us. We would have Russian backdoors in more than 400 of the Fortune 500. And in some of the very federal agencies like Homeland Security and the Pentagon that are supposed to keep us safe, and they didn't even that Russian hackers were inside their system. So this whole incentive structure is so broken. And I think we really need laws and policymakers to step in.

KRISTEN EICHENSEHR: Yeah. It's been interesting in the last few weeks too. There have been announcements from a number of members of Congress who've been really actively engaged on cybersecurity issues that they're going to be retiring. So that knowledge deficit is I think getting perhaps worse, not better.

Let's turn away from ransomware in particular, and I want to talk about-- that's been an issue that's been in the headlines. But there are perennial issues that are lurking behind all kinds of different cybersecurity headlines. And one is the one that you focus on in your book, and that's the market for zero-day exploits.

So let's just start with the basics. So can you tell us what is a zero-day exploit. And how has that market for them evolved?

NICOLE PERLROTH: So a zero-day is-- and I'll just make it-- I'll use a tangible example. If I'm a hacker and I find a bug in your iPhone software, your iOS software that Apple doesn't about, I can probe and pick at that bug and see maybe I can do something with this.

And let's say I was a really good hacker and I could craft a program that could exploit that software bug to read your text messages, to track your location, to record your phone calls, to turn on your camera. That's the zero-day exploit that's really the mother of zero-day exploits.

If you can craft that program and hijack anyone's iPhone remotely, you can sell that right now to a number of brokers. Some of them are based in Washington and Virginia for $2.5 million. If you can do it in Android, if you can get a really good remote zero-day exploit for Android software, that's $3 million now.

And then there are companies overseas in the Gulf that will offer you $3.5 million for that zero-day exploit. The caveat is if you sell that exploit to one of these zero-day brokers, you can never talk about it. Because the minute you talk about it, Apple finds out about it, Apple works on a patch.

We'll get one of those annoying software updates to patch our software, update our software. And suddenly that $2.5, $3, $3.5 million investment goes to dust. Those brokers, their biggest customers are government agencies because you can see how that iPhone zero-day exploit I mentioned earlier, would have tremendous value for spy agency.

I mean, what else do you need? It's basically if you can get into someone's iPhone remotely, you have an invisible ankle bracelet on them. You who they're talking to. You know where they are, you know what they're saying.

So I had heard about the zero-day exploit. I had met with these companies who actively advertised these price lists on their websites. But the thing no one wants to talk about is who their customers are. And I knew that the US government was among the biggest buyers of zero-day exploits.

And that started to gnaw at me, to say the least. I was just in my little perch at the New York Times, here I was with my head cut off like a chicken running from attack to attack all over the globe as they were getting more sophisticated, more destructive. Coming from corners of the globe like North Korea and Iran that we had underestimated in this realm.

And it's not as if we're all using different software, we're all using the same software. We're all using iPhones, and Android phones, and Microsoft Windows, and Linux. And in our industrial systems we're all using Siemens industrial software, or Schneider Electric software.

So when the US government stockpiles a zero-day in one of those pieces of software so that it can spy on terrorists, spy on Russian foreign officials. Embed themselves in the Russian grid through some of that industrial software I just mentioned, they're not just leaving open a hole for our enemies, they're leaving open that hole for Americans too.

And it was no longer hypothetical that our enemies would try and search for those same zero-days, and try and use them against the United States. It had started happening. And to me, this was the one thing-- it was like *Fight Club,* is what I say in the book. It's a one thing no one wants to talk about.

The first rule of the zero-day market is nobody talks about the zero-day market. Second rule the zero-day market is nobody talks about the zero-day market. But to me it was critical to crack this thing open, and really get Americans to understand that their own government-- that as taxpayers were paying government to keep us safe.

But when it came to cybersecurity, we were paying the government to leave us more vulnerable. And really what was happening is we embedded software into everything, was that we were trading on cybersecurity in the name of what we traditionally consider to be national security without admitting that they had become one and the same.

And for the most part, our enemy saw this. They saw that, OK, we might never be able to match the Pentagon spending on traditional weaponry, but for the cost of 1% of a fighter jet, we can buy the digital code to do the United States a lot of harm. And in a lot of cases, they're not coming directly for the Pentagon or Cyber Command, they're coming for where the value is.

They're coming for the companies that run our critical infrastructure like pipelines, and the power grid, and our dams, and our water treatment facilities. 85% of which are owned by private companies that have no regulation whatsoever saying that they have to meet some basic standard of cybersecurity.

And so again, here was a realm where we were designing the most vulnerable system possible. And no one seemed to understand just how vulnerable the United States had become.

KRISTEN EICHENSEHR: The United States government has a process that's supposed to be designed to kind of manage this trade off between keeping a vulnerability secret, and using it for offensive operations or disclosing it to software maker and having it patched. It's called the Vulnerability Equities Process.

Can you say a little bit about what we about that process? And I get the sense, the strong sense that think it skews too far in favor of retaining the vulnerabilities. But can you just talk a little bit about how that process functions as far as we know.

NICOLE PERLROTH: So it's a terrible name. The Vulnerability Equities Process. We call it the VEP for short. So we'll call it the VEP. So first of all, the United States gets tremendous credit for being first government in the world to set up a VEP.

No one is sitting around a mahogany table in Tehran debating whether to keep or turn over a major zero-day in Microsoft software to Microsoft to get it patched, right? That is what the VEP is. Basically it's very much a-- let's just say it's not very transparent.

But it's a process that usually takes place at the White House where various representatives of civilian agencies, and also intelligence agencies, are essentially brought around a table-- I don't what they were doing in the pandemic. But you sit around a table, and they debate whether to keep or turn over a new zero-day discovered.

Usually by the NSA or by one of these zero-day brokers that sold a zero day to intelligence agencies. And in some cases, they do turn them over to the Googles, and Microsofts, and Apples of the world. And in some cases, they don't.

And when they don't, the rules of the VEP dictate that you're supposed to revisit that zero-day periodically to say, do we still need to keep this for ourselves? And there is criteria that government officials say is taken into consideration.

And that criteria is how hard was it to find this zero-day? Is it likely that our enemies would find this and use it back on us? How widely used is the code that it affects? If it's Microsoft Windows, which is some of the most widely used software on the market, we're more likely to turn it over to Microsoft than we would to keep it.

How destructive would this zero-day be in our enemies hands? And again, like do we do we need to keep this in our stockpile for another year, another six months? Let's make sure we're periodically revisiting this. So props go to these ideals, and the criteria we set out for ourselves.

What happened was that in 2016, 2017, someone-- we still don't who they are, but they called themselves the Shadow Brokers, showed up on Twitter, and said that they had hacked the NSA. And over the course of several months, between 2016 and 2017, they started dribbling out the NSA's zero-day exploits.

And I think it was February or March, they dumped the mother of all zero-day exploits. Which was a zero-day exploit that the NSA had code named EternalBlue. It affected Microsoft systems. And what happened next was North Korea picked it up in a global ransomware attack called WannaCry. And it affected hundreds of thousands of systems all over the globe.

Fortunately, they've been sloppy with the code. So a hacker in the UK was able to neutralize the attack pretty quickly. But then a couple of weeks later Russia picked it up. And they used the NSA zero-day exploit in an attack on Ukraine called NotPetya, that to this day is the most destructive, costly cyber attack the world has seen.

It hit every federal agency in Ukraine. It made it impossible to get money out of the ATMs in Ukraine. It made it impossible to pay for gas at gas stations in Ukraine. It affected railways, the postal service. Even paralyzed Chernobyl, the old nuclear site, where they couldn't-- their radiation monitors stopped working, and they had to send people out by hand to monitor radiation leaks using handheld radiation monitors.

But what also happened was it didn't just hit Ukraine, it hit any business around the world that had even a single employee working remotely from Ukraine. So it hit Pfizer, it hit FedEx, it hit Merck so badly that it actually put Merck's survival at stake. Their vaccine production lines, their factories were completely paralyzed in that attack. They had to tap into the CDC'S emergency stockpiles of vaccines that year.

So all told, I think people counted up $10 billion in damage. But that was considered probably an underestimate, because so many of the victims didn't want to admit that they had been hit getting to what we were talking about earlier about the stick your head in the sand, and pretend it didn't happen approach.

When you look at EternalBlue, and you think about the fact that it would have gone through the VEP process, it demonstrates just how broken the VEP process was. How widely used was the software that it had affected. It was Microsoft Windows. So pretty much the most widely used software in the world.

How destructive would it be in our enemies hands? Very destructive. Between North Korea and Russia. It was easy to use, and it cost upwards of $10 billion in damage. How long did they keep it? More than five years.

When I went back and interviewed the people at the NSA that had basically developed it, that is inexcusable. The government still owes those companies a huge apology in my opinion for holding on to that zero-day day, letting it get out. And then letting them get stuck with those damages.

And by the way-- and there was a development on this recently. So I don't remember what it was. But I think it was positive. When those companies like Merck went to their cyber insurance underwriters, and said, OK, we had $500 million in damage. And we have a cyber insurance policy.

Their insurance company said, sorry, we're not going to pay this out. Look at this fine print. We actually have a war exemption in your policy. And we're going to invoke it because you were collateral damage in Russia's war on Ukraine. So we don't have to pay this.

So all of these companies in the United States, some of our most vibrant critical companies were left footing the bill for $500 million, $600 million because of this zero-day day exploit that got out from the NSA. That's what I call a broken system you. And if you just apply what happened in that one attack, and we don't how many other cases there that are similar, but just in that one attack you can see that, wow, we have a lot of work to do on the VEP process.

KRISTEN EICHENSEHR: There's a ton of interesting things in what you just said. Let me pick up on two of them. Let me ask you first about attribution, and then I want to go to Ukraine, which is obviously a dominating a lot of headlines at this point.

But first on attribution. In discussing the cyber insurance market, these exclusions that policies have for hostile and warlike actions seem to depend at least in part, on the attribution of actions to a state. If an attack is attributed to a state or a state sponsored actor, that makes it seem a lot more like a warlike action. Think of states conducting wars. Not always, but that leans in that direction.

As a journalist, how do you think about when to name a state is responsible for a cyber attack. You've done that in some of your articles. I think I mentioned at the beginning, your reporting on the Chinese People's Liberation Army. United States ultimately indicts members of the PLA for these cyber attacks. So can you just tell us a little bit about how do you think about when to name a state is responsible. Whose determinations on that do you look to?

NICOLE PERLROTH: Yeah, it's a really good question. And it's a really tricky question for every journalist that covers cybersecurity. I would say in my first three years at the New York Times I was always very skeptical of attribution claims. How do you what you know? Especially when those attribution claims would come from government officials. Because I'm of this era of the post-iraq war where a lot of the intelligence that came out of that was wrong.

And so you have this really healthy skepticism in the beginning. Then my experience with the PLA attacks really shifted my thinking. What happened was the New York Times was breech. I actually embedded with our security team and with Mandiant, who we'd hired to bring in for several months.

It wasn't clear that I was going to write about it, but I'd actually just gotten a tip from our security team and asked if I could sit with them. And we would watch the guy that we came to call the Beijing Summer intern roll into our systems at 9:00 AM, Beijing time, and roll out around 5:30 PM Beijing time.

And being there with Mandiant, and seeing that the code that was being used was the exact same code that had been used a thousand times by the same PLA unit in thousands of other breaches that they had responded to gave me a whole new perspective around attribution for cyber attacks. These attacks, for the most part-- I would say 95% of the attacks I've covered repeat code. Have repeat tools.

And China, in particular, was probably one of the biggest digital menaces to the United States. Not so much for their sophistication, but for the frequency of these attacks. And so at the end of the day, what I learned not just in our own attack, but later in calling out some of these PLA units was that these private companies knew a lot more about attribution than I had given them credit for.

I mean, eventually when we culled out the PLA unit-- I still remember their number, 61398, we had their bases on their computer screens. They had gone back to the servers that they were using, and reverse engineered it all the way back to their keyboards.

And they were filming some of these guys doing these attacks from inside this building in Shanghai that we ultimately outed. So that just gave me a whole new understanding that, wow, attribution is more possible in this realm than I think the American public understands.

Now, there are exceptions. And also, I should say, one of the biggest nightmares of my time at the New York Times was covering the Sony North Korea attack a year later. Because if you remember North Korea hacked Sony. And there was again, this healthy skepticism at first.

Well, is it really North Korea? Are we sure it's not an insider? Isn't this Judy Miller's stuff. Iraq war stuff? And from our vantage point, no. The intelligence agencies were saying this is North Korea. Obama was getting on television saying this is North Korea. He'd never done that before.

But where I was betting it was with these private forensics firms who were saying this is the exact same code that was used in an attack on the South Korean media and banks-- media organizations and banks two years earlier. And this is the exact same code. They're using the exact same wiper tool.

And so when you take all of that together, you see that attribution in some ways it's science, but in some ways when you look at the totality of evidence, it's a little bit of an art. And in this case, you have two completely different sources of intelligence and forensics telling you the same thing, and pointing to these tools. You can be pretty confident in the attribution.

So we were reporting that and every time there is this bothsidesism to media. Every time we would say this is North Korea, there would be another journalist saying, but is it? And I think generally it's good to have that pushback because it pushes these forensic investigators, and government, and intelligence agencies to make sure that they can provide evidence for it.

But it's tricky. And what is interesting to me is that in recent years, we've actually caught Russia playing around with attribution. So they hacked-- there was a hack on French television networks that took out these television stations and put up pro-isis propaganda. So you assume it's ISIS. OK, a year later we learn, no, it was the GRU. It was the-- it was these Russian-state backed hackers.

The opening ceremony at the Olympics in South Korea. The opening ceremony was hacked. So people couldn't actually get in because the ticketing system had been hacked. And so when you looked at who was sitting around the stadium at the opening ceremony in South Korea, it looked really empty.

And given the target, South Korea, we all assumed, OK, it's probably North Korea. And in those early stories if you go back and read them we had a lot of skepticism. We don't who this was, but someone just hacked the Olympic ceremony. A year later we learned, no, it was the GRU again. Apparently upset about the doping restrictions.

There was one other where we actually caught them, the GRU hacking into Iran's command and control servers. And using Iran's attack infrastructure for their own attacks. So that's interesting.

And then there's the one that keeps me up at night, which was an attack on Petro Rabigh, which is a Saudi petrochemical facility where someone broke in, they used all custom code. So this falls into that 5% exception category where they weren't reusing any code. They broke in and using all bespoke code, and zero-days, and Schneider Electric software, neutralized the safety locks at the plant. The very last thing that prevents an explosion.

And given the target, a Saudi facility, petrochemical facility, the initial suspect was Iran. Because Iran for years had been hacking these Saudi Aramco, and a bunch of Saudi oil facilities.

And again, fortunately because it was all custom code, the way we framed it was someone hacked this petrochemical facility in a very disturbing way. Potentially a very destructive, almost cyber terrorist way. But they used all custom code, and we don't who it is.

And it took a year but researchers actually traced it back to a graduate research University outside Moscow. So my rule has always been if they're reusing code, if they're using tools. If they were able to trace it back to command and control servers that had been used by a nation-state and a number of other attacks.

And if I'm getting some confirmation from intelligence sources of what the private sector is seeing, then I think you can be fairly confident in at least saying, the evidence suggests that this is who is behind it. But, caveat here. And then there are cases where you just say there was a very sophisticated attack that used all custom code. It was in Saudi Arabia. Obviously, the suspect is Iran, but we've never seen this kind of attack from Iran before. And then you wait until someone has actually pinpointed the building that it came from.

So that's sort of how I've handled it. And it hasn't always been perfect. There was a case where there was a hack of JPMorgan. And everyone inside JPMorgan and law enforcement was saying this was Russia. And I don't think we ever said that. But we said the suspect-- the thinking is that this was a nation-state.

And then later turned out, no, it was two guys in Florida. So that really gave me even more skepticism that actually there's a weird incentive for banks and targets to pin this on a nation-state. Because it suggests that, oh, this was so sophisticated. We could have possibly done anything to prevent it, rather than it was two guys in Florida. We really don't who did this. We'll see.

KRISTEN EICHENSEHR: It's interesting we have seen that for a long time of victims want it to be the sophisticated attack against which they couldn't possibly have defended. But then there is this cyber insurance possibility hanging out there that the more sophisticated, the more they attribute it to a foreign government, the less likely perhaps it's covered by insurance. So there's a little bit of a tension there.

But let's talk a little bit more about Russia and Ukraine. Obviously we're at a moment of tremendously increased tension over Ukraine, and fears that Russia is going to invade. Russia has used Ukraine as a bit of a test range for cyber attacks in the past.

Attempting to change election results. Shutting down electricity grids. Obviously NotPetya, which you mentioned. What would you expect to see over the next couple of weeks. This is perhaps a little bit of an unfair question, because the big question being is actually going to invade or not? But on the cyber front, what do you think Ukraine is particularly vulnerable to?

NICOLE PERLROTH: So I have to be a little bit careful about how I answer this question, which is a new one for me. Because in December I joined CISA's advisory board. So as part of that, I do get classified briefings now. So I have to be a little bit careful about what I say.

So what I'll tell you on this recorded line is what I've already reported. So I've already reported some of the attacks you mentioned. Russia has used Ukraine, as you say, a test range. I call it a Petri dish. They've tested out everything in their arsenal on Ukraine.

They have shut off the lights. They've shut down the ability to get gas, to get money out of ATMs. They've shut down railways and transportation systems. So we they're capable of that. And if you were to invade a country, and you've already tested all of those things out on them, why wouldn't you do that first?

And make sure that it's really hard for various government agencies to communicate with each other. Why don't you put pressure on large demographics to just roll over because you're sick of the power being off, and unable to get gas. And all of the critical things that we now depend on for our survival and for innovation.

So to me it would be a no-brainer in general for a nation-state with those capabilities to deploy them before, or timed to any invasion. I think what people need to remember. And again, this is an open source of my own reporting, and it's in the book, Russia has been hacking into our critical infrastructure for a very long time.

For the last decade-- actually, more than a decade now, I have reported that they have hacked into our power grid, into our energy companies. Into our-- well, I don't think I've reported that one. But they've basically hacked our critical infrastructure. They probed our nuclear plants. They probed Wolf Creek, which is a nuclear plant in Kansas.

And Putin has said, if the United States were to get involved in Ukraine, that would be crossing our red line. The red line terminology is very interesting, because that's not a Russian phrase. There's no easy translation. For that that's an American, diplomatic, military term.

And so he throwing it back on us and saying, if you respond here in an aggressive way, you'll be crossing our red line. And I think the best way for Putin to fire back on that would be to use the access that Russia already has, in many cases, to inflict harm on the United States.

And that gets back to my previous point at the beginning of the session, which was we are so vulnerable. We have been hacked over and over again. Our most critical systems are held by private companies that haven't even admitted that they are attacked.

And when it comes to traditional military defenses, the United States major advantage has always been we're an island of our own, in many cases. We have two oceans protecting us. But when it comes to cyber attacks, there's no island. There's no oceans.

And it would be very easy for the nations, or the world's savviest cyber predator to use access that they already have as a lever in this kind of military escalation. And so I am freaked out to tell you the truth. I'm totally freaked out by what's happening in Ukraine.

And I don't if Putin's even decided whether to invade, or what levers he's going to pull. But that the levers are there. I don't think that the American public even understands the kind of damage that could be inflicted by cyber attacks here.

KRISTEN EICHENSEHR: OK. So that's distressing, obviously. Let's pivot away from the interstate politics aspect of this for a minute. I want to talk about another way-- something else you talk about in your book. It kind of takes us down to the individual level, and that's the use of surveillance tech against individuals. Against journalists, against dissidents.

You talk in the book about-- you wrote some of the early stories on this issue, and you talk in the book about older players like Hacking Team. But this issue has really now, I think, become pretty synonymous particularly in the last six months or so with Israel's NSO group.

The Biden administration has done a bunch of things recently to try and crack down on some of the software. So putting NSO group on the Commerce Department's Entity list. Taking actions against Chinese companies that enable surveillance against the weaker minority.

Can you talk a little bit about what does that market look like, and what do you think of the efforts the Biden administration has been taking? Will these be effective at shutting down that version of the threat against individuals?

NICOLE PERLROTH: So what that market looks like is companies like NSO sell click and shoot spyware to government agencies. And basically, you would not need to have, really, any technical or hacking skills. But if you buy this product, if you buy NSO's Pegasus product which is the technology that spies on mobile phones. It's sort of a push a button and you're in kind of thing.

And for a long time victims knew that they were getting targeted with NSO, and would call me because they were getting strange SMS text messages. That says you your child's in danger. Did you see this news headline? Did you see your mention in this news headline? And people would click and it would take them to Gayosso, which is a Mexican funeral website.

And so clearly they were clued on to something as is weird here. And then they would come to me or they would come to Citizen Lab. And we would confirm that, oh, yes you were hit by NSO's Pegasus spyware.

Then there was this disturbing turn where NSO started selling a zero-click capability, which means that there's no SMS text message. There's no Warning. Governments don't have to do anything. They just click the button, and they're inside your phone. They use zero-day exploits to get inside your phone. Some of that uses maybe a series of zero-days in iOS software, Android software, or maybe it's just one. But they leverage zero-day in a lot of cases.

So NSO it's an Israeli company. It was started in 2010. They said that they require Israeli government authorization to sell those tools to any foreign buyer. They told me they had a whole human rights-- call it a filter, I guess, that they would put their customers through, or would be customers through. Or they would say, where does this country fall on the MNIST international list of human rights abusers. If they're low on that list we won't sell to them. If they're high on that list, then OK.

But over and over again, their spyware was showing up on the phones of dissidents in the UAE, journalists in London. And then I covered a series of really disturbing cases in Mexico, where the NSO's spyware was showing up on the phones of journalists, but also nutritionists. Which was a weird one.

And we found out those nutritionists had dared advocate for a national soda tax at some point. And so someone in government was using this government spyware to get into their phones maybe because they were getting Kickbacks from the soda industry. Who knows? What was clear is that this was totally out of control. There was no oversight.

And these are really intelligence tools that in the hands of governments that don't have a process to protect human rights, and to protect from the abuse of human rights, I should say. They could be very powerful tools for corruption, and abuse. And to suppress dissent, and to clamp down on a free press.

And so that's basically what I've been covering for the last 10 years, was just abuse after abuse. First from Hacking Team, and Gamma Group, and some of these companies in Europe. Where Europe very quickly clamped down on them. And then later, NSO group, where Israel did not quickly clamp down on them.

And then what happened is in the Biden administration, there was just some great reporting for my friends at The Times, Mark Mazzetti and Ronen Bergman, that said actually the FBI was considering buying Pegasus zero-click spyware last summer, and then didn't because of the questions around ethics and human rights abuses, and some of the reporting.

And then late last year in November, something happened that I never thought I would see, which was the Biden administration. And really, a remarkable breach with Israel, our Israeli allies, blacklisted NSO group. And basically destroyed their chances of a profitable exit. They had been planning a $2 billion IPO, I think. And this destroyed any chance of that.

And also sent a really powerful message to governments elsewhere that, hey, we will act if you're caught selling spyware. Someone in your country is selling spyware that's being used to abuse human rights.

So overall, I think it's a really positive step. It's probably an overdue step. But since then in the last month or so, there has been new reports. And I apologize, I forget who reported this-- of new Israeli companies that we'd never heard of, caught using spyware on the usual suspects.

And this was always Israel's argument was if it's not us, then you're going to see the spyware come from countries that aren't going to have any human rights process in place, no filter in place. Aren't going to check that these buyers are human rights friendly. And this market's going to go to the Chinas and Russias of the world.

So ultimately you'll be doing yourself a disservice. And now we're seeing these companies come out of Israel. So there's new companies to consider blacklisting. And it's going to be a whole whack-a-mole thing. And you can see how China would become the ideal headquarters for this industry. And so I think that's probably going to be the story over the next decade.

KRISTEN EICHENSEHR: Let me ask you one question we've gotten from the audience that relates to something you said earlier in the discussion, which is about requiring reporting of incidents from companies, but also giving them liability protection. And so the questioner asks about the effect that this would have on companies stock prices.

And putting them in this position where they have to disclose, but then they get hit in the stock prices. Can you talk a little bit about what effect you've seen on companies that have disclosed these major breaches afterwards? Does it actually hurt them in the long run?

NICOLE PERLROTH: Yeah and that's a really good question. Because there's no doubt in some cases, it would affect their stock price. Now, the reality is sort of sad. But I would cover these attacks. The one that really comes to mind is Home Depot.

There was a really egregious attack by cybercriminals on Home Depot years ago. And I covered it not just that it happened, but I went deep on some of the trade offs the company was making on security in the name of cost. Or they were just cost cutting, and so they never-- any dollar they could have spent on security, they weren't spending because of cost considerations. And people were even in the security department, were you even telling their family members only to use cash at Home Depot. I mean, it was that bad.

And so I laid this all out in a story with my colleague. And I thought, wow, this is really-- I feel almost bad for Home Depot. This is really going to affect their stock price. And I think there might have been a teeny little dent that day that the story came out, and then it just kept climbing.

I mean, that is the weird thing about breaches, is the market in many cases, doesn't care. The only time we've really seen the market care was when Yahoo was acquired by Verizon. And then it came out after the fact that they had been breached twice by Russian hackers, cyber criminals, and the FSB, a KGB successor.

And Verizon ultimately docked their acquisition price by, I think, $200 million. That was the first time we saw any real market penalty for a breach. But other than that, for the most part, we traditionally just see a minor dent, and then things keep going. And I think that has to do with the fact that a lot of people just don't care.

KRISTEN EICHENSEHR: And so many companies have been hit. The stigma is dating, it seems like, perhaps. So let me just wrap up here. We've only got a few minutes left, by just asking you to look forward a little bit. I mean, it feels like with cybersecurity reporting and the legal issues, we kind of go through these eras.

For a while everyone talked about intellectual property theft, and we talked about election interference. Now we talk about ransomware. So can I ask you to just kind of forecast forward for us what are the cluster of events or issues that you would expect a year from now, two years from now-- we'll keep it on that narrow horizon, because eras in cybersecurity move fast. But what do you see coming down the line?

NICOLE PERLROTH: Well, I don't think intellectual property theft will go away. It just makes a lot of sense for a lot of countries that they're never going to have the R&D spending that we do in the West. And so if they want to become an innovator, and they don't want to spend that money on R&D, why not just steal the R&D. And that has been the story of China for a long time. And I think will continue to be the story there.

I unfortunately think that we will just continue to see a lot of sabotage and destructive attacks. I think they'll be tied to these geopolitical events that are escalating. Maybe it's Ukraine, maybe it's Taiwan. But I think at this point it's safe to say that any future geopolitical conflict that escalates to a war, or just short of war, will involve some cyber elements to it.

And I think the country that will win those conflicts are countries that look like a digital Israel. A country that can basically continue to run basic critical services, and innovate while surrounded by hostile neighbors, and hostile activity. And right now the United States is not that country. We would lose several of those conflicts.

And so unfortunately, I think over the next decade, depending how things escalate-- because there are a lot of hot points around the world right now. I think, unfortunately, we're due for some short-term pain when it comes to cyber sabotage, attacks on our critical infrastructure. Attacks on those companies that run our water, and power, and pipeline systems.

And only then I think will congress be forced into action to raise the bar, raise the minimum standard for cybersecurity. That will make compromises on privacy in the name of cybersecurity. And that will be interesting when that plays out.

And then I think we'll continue to see these attacks get more sophisticated. So those sloppy Chinese attacks I was covering back in 2010 to 2012, they're not sloppy anymore. They used to be spear phishing attacks, now they're zero-day attacks. There's new laws that have been put in place in China over the last year and a half that have told Chinese researchers who are some of the best we see at hacking competitions every year in Vancouver. That have told them, you can no longer go to Western hacking competitions.

If you find a zero-day you have to give the state right of first refusal. And how is that playing out? It's playing out in the fact that over the past 12 months, we've seen a record number of zero-day attacks come from China and they've been very aggressive, and very hard to catch because they use zero-days. And so I think we're going to see more of that.

And I hope by the end of the decade that short-term pain will have reached the threshold where will be ready as a country, and as a world, to set up international norms for cyber behavior. And to lay out what is acceptable, and what is not acceptable. And figure out ways to enforce those rules.

I mean, unfortunately right now the United States would never agree to something that sounds like a no-brainer on its face, like a digital Geneva Convention. Of course, it sounds great that we would all agree, hold hands, kumbaya, and agree to not hack each other's hospitals, and power grids, and water supplies.

The problem is that all of the attacks that the United States conducts come out of Cyber Command, or if it's espionage it comes from the NSA or one of the intelligence agencies. That's not the case in China and Russia. They regularly outsource these attacks to private citizens in China's case, or to cyber criminals in Russia's case.

And so how do you set up these international norms for a transnational realm where so much of this behavior that comes from our adversaries comes in the form of proxy attacks. And after the NotPetya attack, or maybe just before it, I'll never forget. Putin said, hackers are like artists. They just wake up in the morning and a good mood and start painting.

In other words, I have no say over what they do or don't you. So the US position is, how do you come to some international digital Geneva-like convention agreement with that guy? [LAUGHS] And I think that they are right.

I don't how you do that. I don't how you hold our enemies feet to the fire. Maybe we get to a point where we say any attack that comes from inside your borders will hold you, the state, to account. But then what do you do if that Russian cyber criminals living in Ukraine, or Romania?

Or that North Korean cyber criminal is living in China. It's so messy. It's so hard. But I think it's not so hard that it's impossible. And I think too often we treat these issues as impossible-- it's so hard, it's so impossible, we'll just figure it out down the road. And Meanwhile, the attacks keep getting worse.

There are more attackers than ever. There are more countries that have these capabilities. They say now that there is no country on planet Earth with the exception of Antarctica that isn't trying to acquire zero-days, and offensive cyber tools for its own attacks, and its own espionage.

And so we have to come to terms with that world. And we have to come to terms with our own vulnerability. And then we have to start plotting ahead.

KRISTEN EICHENSEHR: Well, thank you for that. That's a great place to wrap up on the role and work that we have to do as citizens, and also as lawyers, since many of our audience are lawyers or budding lawyers. So thank you very much for sharing all of your expertise with us today. I really enjoyed the conversation, and appreciate you being here. Thanks, Nicole.

NICOLE PERLROTH: Thank you so much. And thank you to everyone. And I really do believe that solving this problem, it's not a technical problem anymore. It's a whole of society problem. Don't think that have no place in solving this because you're a lawyer, or you're not technical. You have a big role to play. Arguably, more of a role to play.

And so please, please, the reason I do these talks is because I want people to get involved. And I want to see new ideas for how to contain this. And the old ideas aren't working, so I think it's time to bring in more outsiders. So thank you. Thank you for listening. And thank you for having me.

KRISTEN EICHENSEHR: Thank you very much.