Gaslit Nation
Dec 25 2019 Transcript

Sarah Kendzior: I'm Sarah Kendzior, the author of the bestselling essay collection, *The View From Flyover Country*, and the upcoming book *Hiding in Plain Sight.*

Andrea Chalupa: I'm Andrea Chalupa, a journalist and filmmaker, and the writer and producer of the upcoming journalistic thriller, *Mr. Jones*.

Sarah Kendzior: This is Gaslit Nation, a podcast covering corruption in the Trump Administration and rising autocracy around the world. We are an independent podcast supported by our listeners and we encourage you to sign up for our Patreon, to keep the show going and to get extra episodes and bonus features. Today, we have a special guest interview. Andrea, do you want to tell us about that?

Andrea Chalupa: Yes, so we have on the show the full interview with WIRED Magazine's Andy Greenberg, talking about his new book, which is a real-life science fiction. A little of real life. Okay. It reads like a science fiction political thriller. It's called *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. This is an essential guide into one of the greatest challenges of the 21st century cybersecurity and cyberwarfare. It's just thrilling. You have to get your hands on this book. It'll give you X-ray vision into the news cycle and where events are headed.

Sarah Kendzior: All right, so here is Andy Greenberg.

Andrea Chalupa: Welcome to the show.

Andy Greenberg: Thanks for having me.

Andrea Chalupa: I am freaking out right now inside because I had been digging into *Sandworm*, and I have to tell every single listener of the show that *Sandworm* is required reading. If you want to understand how we got here in the world today and where we're headed, if you want to read through the headlines, if you want to see the next steps that are coming in this chaotic news cycle, you need to read Andy's book *Sandworm*, just to have an essential framework on to some of the most dangerous issues that the world is facing today. This is something that Sarah and I talk about a lot privately. We don't have the expertise in cybersecurity, of course, to do a lot of this coverage on this show, which is why we're thrilled to have you on and to pick your immense brain and knowledge about this critical issue.

Andy Greenberg: Well, that is super kind. I have admired this show because you guys have had this really admirable focus on Ukraine among other things, and that happens to be the subject of this book. This is a story about a cyberwar that unfolded in Ukraine that the world has watched unfold without reacting, without coming to the defense of this country in the shadow of Russia. As a few, Cassandra has warned that this cyberwar was going to spill out to the rest of the world, and it did. That is the arc of the book. By the time that we felt the effects of this cyberwar in the West, it was too late. I think that you guys have told the story of Ukraine as something of like a canary in a coal mine for the West, and this story kind of mirrors that as well.

Andrea Chalupa: Absolutely. When I was reading it, I was reminded of one of my favorite books that I read as a kid and that was Kurt Vonnegut's *Cat's Cradle*. You essentially wrote like Kurt Vonnegut's *Cat Cradle* here with *Sandworm*.

Andy Greenberg: I would not claim to have written any kind of Kurt Vonnegut ... anything. He's amazing, but ...

Andrea Chalupa: [inaudible 00:03:27] gripping. The irony is there.

Andy Greenberg: It's funny that you say that because in the climactic moment of this story of these military hackers, these Russian hackers release a worm called NotPetya in Ukraine that is designed to devastate the country, that spreads to the rest of the world, becomes the worst cyber attack in history. Cost was $10 billion in damage. Shuts down hospitals across the US, this largely untold story. It's so analogous with the Ice IX part of *Cat's Cradle,* this kind of military blindness that you can just create this thing that spreads virulently, turns water into ice, and of course, it causes an apocalypse. Anyway, I would never compare anything I write to *Cat's Cradle*, but you did it. So I'm allowed to say that.

Andrea Chalupa: Well, I'm just saying it's an engaging book. I was reading *Sandworm* on my couch, my husband was nearby watching TV and I just kept gasping, gasping as I was turning the pages of your book. I'm not normally that vocal when I read, and my husband's like, "What is it? What is it? What's going on?" I'm like, "This book is incredible." I know I'm known for my enthusiasm on this show, but I am genuinely, I am obsessed with this book and I think it's absolutely required reading because you also go into the essential history of Ukraine, and as we're always saying on this show, you must understand history because we're not just living in these events that happened overnight. It's a continuation of conditions that have been going on, persisting, in some cases, over many centuries. As I've always said, it's a miracle that Ukraine as a country even exists. And you give us an essential overview on Ukraine's history and why it matters today.

Andy Greenberg: I was trying to kind of write it as a detective story almost. But I do try to go into that Ukrainian history because the story of Ukraine is so important. It has always been caught between East and West. It is the borderlands. As a result, among other things, it has become this place where Russia does what it wants to do, where it shows its intentions. In the 21st century, the way that that's expressed itself is in these acts of cyberwar experimentation. That was how I got brought into this story. I became aware that Russian hackers, I didn't know yet who they were, were carrying out acts of cyberwar in Ukraine that they were not doing anywhere else in the world. First, to start, Russian hackers tried to spoof the results of the Ukrainian election in 2014, two years before they would meddle in the US election.

Then, as I was reading about that, a linked group of hackers, in fact, were carrying out the first ever blackout attacks in Ukraine, turning off the power to hundreds of thousands of Ukrainian civilians, first in December of 2015, and then again in December of 2016. I assembled in my head this syllogism. We just watched Russia hack the Ukrainian election and then they hacked the US election. Now we're seeing them hack the Ukrainian power grid. Are we going to see them hack power grids in the West? Are we watching a kind of experimentation and building of capabilities that Russian hackers will use on the rest of the world? That was the first big story I wrote in the series of stories for WIRED that first inspired the book and that were excerpted from it.

That first piece was basically about this idea that what happens to Ukraine should not be ignored because it will sooner or later hit the rest of us. Bizarrely, the day that that cover story for WIRED about the Ukrainian cyberwar hit newsstands was when NotPetya hits this cyber attack that very literally hit Ukraine and spread to the rest of the world. It was a prediction that came true almost too fast. I don't think people even had a moment to recognize what we had predicted before it came true.

Andrea Chalupa: That's totally what we say on the show is that the bad guys are faster than the good guys. Also, Ukraine is a laboratory, a testing ground for Russia's aggression. We've seen that again and again. Ukrainian soldiers right now are going up against heavy machinery and Putin's invasion that no US soldiers had to fight against. So, it's the heavy machinery as well as cyberwarfare. They're both tools that are being tested on Ukrainians, which is why knowing the country, using it, depending on it as a framework, to understand Putin and Putinism, whatever comes after Putin because it's going to be very difficult to get rid of what he's built up. Ukraine is essential to understanding Kremlin aggression generally. I want to ask you to read from your riveting book *Sandworm*.

Andy Greenberg: Yeah, sure. This is the introduction. "On June 27th, 2017, something strange and terrible began to ripple out across the infrastructure of the world. A group of hospitals in Pennsylvania began delaying surgeries and turning away patients. A Cadbury factory in Tasmania stopped turning out chocolates. The pharmaceutical giant Merck ceased manufacturing vaccines for human papillomavirus. Soon, 17 terminals at ports across the globe, all owned by the world's largest shipping firm, Maersk, found themselves paralyzed. Tens of thousands of 18-wheeler trucks carrying shipping containers began to line up outside those ports' gates. Massive ships arrived from journeys across oceans, each carrying hundreds of thousands of tons of cargo, only to find that no one could unload them, like victims of a global outbreak of some brain eating bacteria, major components in the intertwined automated systems of the world seemed to have spontaneously forgotten how to function.

At the attack's epicenter in Ukraine, the effects of the technological doomsday were more concentrated. ATM and credit card payment systems inexplicably dropped offline, mass transit and the country's capital of Kyiv was crippled. Government agencies, airports, hospitals, and the postal service, even scientists monitoring radioactivity levels at the ruins of the Chernobyl Nuclear Power Plant, all watched helplessly as practically every computer in their network was infected and wiped by a mysterious piece of malicious code. This is what cyberwar looks like. An invisible force capable of striking out from an unknown origin to sabotage on a massive scale, the technologies that underpin civilization."

Andrea Chalupa: *Cat's Cradle*. Ice IX.

Andy Greenberg: What I was trying to capture in that intro was we read these hypotheticals at the beginnings of stories and books all the time that say, "What if we shut down dozens of banks? Or what if we turned off the power grids? What if hackers carried out these kinds of attacks on the fundamental infrastructure of civilian life." But in this case, it actually happened, and the world almost didn't take notice. That's what I've been trying to bring to light in this story that there was, in fact, the closest thing we've seen [inaudible 00:09:57] cyber apocalypse, if you want to call it that, that costs $10 billion, it shut down hospitals and power grids and transportation and the private sector and the media and government agencies, and the worlds barely noticed because it largely hit Ukraine.

Then because there was almost a kind of sweeping under the rug of this that happened in the West that, this hit Maersk and Merck and FedEx and all these other massive companies, but they didn't want to talk about it. It took a lot of reporting to bring to light the full scale of those attacks.

Andrea Chalupa: Right. It's one of those hackings generally, whether it's hacking our election systems or hacking our infrastructure. It's one of those shrouded issues that the authorities don't want to share with the public and so the public is left reeling saying, "Look, our votes are at stake, our livelihood is at stake, our security is at stake. Please tell us what's really going on." With all of your many years of reporting on this, tell us what's really going on.

Andy Greenberg: Part of the story, as you say, is that two administrations–the Obama Administration is complicit here, too–ignored an unfolding cyberwar in Ukraine, and treated it as Ukraine's problem. But that story, it starts, in fact, in 2014 when a small company, iSight Partners in DC, discovers that there was a campaign of what they thought was espionage by this group called Sandworm. They call them Sandworm because these little references in their code that they used to track their victims are taken from the sci-fi novel *Dune*. This group, Sandworm, seemed to be infecting NATO targets, Eastern Europe. That was typical Russian espionage. But then they see that these apparently Russian hackers, because they even found Russian language documents on a server these hackers use, were also targeting the American electric grid.

When I learned about that, I could see that this was a story that was not some sort of foreign case study about Ukraine. The same hackers that would later in 2015 and 2016 turn off the power to hundreds of thousands of civilians, had planted the same seeds of those cyber attacks in the US grid. That was my introduction to this story, that I could see that Sandworm was going to be a group that should matter to an American audience. In 2015, after Putin's invasion of Ukraine, began this escalating cyberwar that first started with these data destructive attacks on Ukrainian media companies and transportation and government agencies, and then culminated in the first ever blackout caused by hackers, then hit again in 2016 with this second wave of attacks that led to a blackout in the capital of Kyiv. Then finally climaxed in this NotPetya attack that hit in the summer of 2017.

Each one of these steps was a crossing of a red line where first the Obama Administration and then the Trump Administration failed to call out these hackers who were visibly, for any cybersecurity analysts, doing acts of hyper aggressive cyber sabotage that we had not seen anywhere else in the world, and that deserved recognition, that deserved rebuke and punishments. Yet, were just kind of treated with impunity because it was not our problem, it was Ukraine’s. They're not even in NATO. That is the story that I heard. In fact, when I interviewed officials in the Obama and Trump White Houses, who, for years, failed to act on this escalating cyberwar until it cost US in the West untold billions of dollars, and maybe even a difficult-to-measure toll on Americans' health because hospitals were affected by NotPetya as well in a way that's hard to exactly quantify.

Andrea Chalupa: Well, your book makes it so clear that even the authorities in charge have a difficult time wrapping their heads around this, including the dollar sign of the damages, potential damages and so forth, because it's like our election systems, which is a hodgepodge, a big random quilt of systems. So, too, is our grid. Essentially, you have these governing agencies, but to get them to do any action, there's just so much bureaucracy and hierarchy and so forth. Your book shows through these incredible characters, these cybersecurity experts or turned cybersecurity experts, either in the private sector and the government that were on the front lines of watching Sandworm emerge and trying to do something about it, and they're met with government bureaucracy and so forth at every turn.

What we always say on this show is that Donald Trump being President, that's a story of institutional failure that went on for several years. Especially under the Obama Administration, which like you said, Ukraine was not a NATO partner, so Ukraine was just some poor country over there, and we've got our other priorities. So, if Donald Trump is President of the United States, with the help of the Kremlin, something was wrong with your foreign policy. Could you talk a little bit more on the specifics of the opportunities that the Obama Administration had and how they failed those opportunities to confront this issue?

Andy Greenberg: Well, the Obama Administration, to its credit, it did call out hackers who were crossing red lines in general. Michael Daniel, the cyber coordinator for Obama, his top cyber security official that I spoke to, and he takes pride in the fact that his administration called out North Korea for attacking Sony. They called out Iranians for hacking US banks. They eventually called out Russia for hacking the US election, although a bit hesitantly took a little longer than I think anybody would have liked, but they never called out Russia for attacking Ukraine. That was an implicit signal to Russia that you can do what you like digitally, at least in Ukraine. If I understand, you are a better historian of Ukrainian politics than I am, but there were serious sanctions against Russia for its physical invasion of Ukraine.

But everything after that was a kind of freebie. I think Putin and the GRU, the Russian Military Intelligence Agency, knew that they could get away with everything else on top of that because they'd already paid the price for their invasion. That allowed them to turn Ukraine into this punching bag and guinea pig for all manner of cyber attacks. The Obama Administration, I think, failed to see that clearly, failed to respond, kind of in a typically maybe overly restrained, overly contemplative way, just never acted. Whereas, as that cyberwar escalated, then the Trump Administration took over, it's harder to say why the Trump Administration failed for so long to act.

One thing I heard from Rob Lee, who was this central character of the story and a former NSA hacker hunter who tracked threats to American critical infrastructure, he described going into the White House and giving a briefing on one of these unprecedented pieces of malware that caused the blackout in 2016 in Kyiv and thinking that that would result in some sort of public statement from the Trump White House. But then hearing back that, you know, we're just not interested in doing that right now. I think that you can imagine that it's very difficult to walk into the Oval Office with Trump as President and talk about Russian hackers. We've seen reports that is just a nonstarter of an issue with him. He is allergic to this topic. The result is that he has a massive blindspot to this incredibly important issue to an actual danger to, not just Ukraine, but the global order.

Andrea Chalupa: Yeah, lives are literally at stake right now because the President's ego can't handle adult conversations around the threat of Russian hackers.

Andy Greenberg: I have to imagine that that is what prevented, in part, the Trump Administration from acting after the Obama Administration's failure to act. I have to say that the Trump Administration, or maybe some adults in the White House, did manage to call out Russia in February of 2018 after this $10 billion cyber attack, after it was too late, to say that NotPetya, this cataclysmic cyber attack, was the work of the Russian military. A month later, the White House did impose new sanctions on Russia. That came nine months after NotPetya. That was the kind of inertia of this White House. That's how long it took to recognize an act on the worst cyber attack in history. That came, in fact, years after the beginning of this cyberwar that should have, from the very beginning raised a red alert in the

White House, first for Obama and then Trump, that something was happening that needed to be stopped, needed to be called out, needed a reaction like sanctions or indictments from the very beginning.

Andrea Chalupa: I'm going to read a passage from your book on that character that ... I'm sorry to say character, but your book does read like a thriller, a real-life thriller of major geopolitical consequences.

Andy Greenberg: Well, thank you. I'm very willing for you to call them characters, but I hope that they're not [inaudible 00:19:00].

Andrea Chalupa: Yeah, of course. I'm going to read a passage on a very valuable source for your book. Robert Lee, who is, as you mentioned, a cybersecurity expert that did work in the US government for a time and he was essentially forced to go private, because as anyone who's ever worked in a big corporation, whether private or an organization in the government, the more passionate, as they call it, passionate people have a difficult time in big organizations in really getting things done, especially when they're Cassandras, as Robert Lee is. So I'm going to read from your book.

"Naturally, Lee began asking around about who in the NSA was responsible for tracking hackers that threatened the security of industrial control systems. He was shocked to discover there was no devoted group with that mission. The NSA had teams tasked with finding and fixing vulnerabilities in industrial control system equipment. It had, as Stuxnet would expose," which was the American cyber weapon essentially, that we unleashed in Iran to shut down their nuclear capabilities for that time. "It had, as Stuxnet would expose, its own offensive teams that invented infrastructure exploitation techniques. It didn't, however, have a team assigned exclusively to hunting the enemy’s infrastructure-focused hackers. So, Lee offered to create one."

"He was amazed at how little bureaucracy he confronted. Creating the agency's first industrial control system threat intelligence team required billing out one form, he remembers. So, Lee says, ‘I became the lead of all of industrial control system threat discovery for NSA overnight.’ He was 22 years old, and he says, ‘Pretty fucked up, isn't it?” I would say so.

Andy Greenberg: In some ways, this story is about how the NSA pushed forward the offensive elements of the cyberwar arms race without sufficiently focusing on defense. That's a story we've heard for a long time, but as you touched on in that passage, this began, in a way, with Stuxnet, this very first piece of malicious software the world had ever seen that reached out from digital systems to destroy physical equipment. Stuxnet was this kind of virtuosic piece of malware that the NSA and Israeli Intelligence together created that was designed to infect the Natanz nuclear enrichment facility in Iran and destroy the centrifuges that they were using to enrich uranium to make a bomb.

The worthiness of that mission is debatable. That may have, in fact, prevented Iran from creating a nuclear weapon and may have prevented Israel from trying to bomb that facility with an actual air strike, it may have prevented a physical war. But at the same time, this piece of malware that, for the first time ever, could destroy stuff in the physical world, it unleashed, it unlocked Pandora's Box. We are now seeing what is coming out of that box, and Sandworm is the first group, since the NSA and Israeli hackers who built Stuxnet, to build malicious software that reaches out from the internet to mess with the physical equipment of the real world to turn off power, and ultimately, with NotPetya, to shut down massive swathes of the world's physical infrastructure.

Andrea Chalupa: This nuclear bomb 2.0, essentially that's what we're dealing with. It's amazing how much it reflects the rise of the nuclear bomb. The US is the first to unleash the Pandora's Box and Russia quickly catches up with its own nuclear bomb. So now we've gone nuclear essentially with cyber.

Andy Greenberg: Yeah. I hesitate to compare it to nuclear weapons because nuclear weapons do kill hundreds of thousands or millions of people. We have not yet confirmed a single actual death from a cyber attack. That's not what you're saying, of course, but your point is true, that we're tempted by this technique. Michael Hayden, the former Director of the NSA, called Stuxnet something like a kind of "*1945* moment" when we've seen the new weapon unleashed and it has changed the world forever. Five years later, we saw Russia begin to use the same tools, as you might expect from Russia, they're using it in a less restrained, less targeted way that does not distinguish between military and civilian targets. They're willing to cause massive collateral damage and the results have been catastrophic.

Andrea Chalupa: That's what they do. The Kremlin deliberately bombed civilians in Syria. We've seen that again and again. At one point, a human rights group on the ground in Syria that works with the UN said that Putin killed– this is under the Obama Administration–Putin killed more civilians in Syria than even ISIS. The way the Russians carry out their destruction is they don't care between civilians and military.

Andy Greenberg: Yeah. This story for me is about the two sides of this that the Russian government is absolutely callous in their reckless disregard for civilian life, but then the West, and especially the US, has been negligent and blind to this problem and also driven it forward with our own kind of sense that we can use these tools for our purposes without the enemy using them against us, and of course, they do sooner or later.

Andrea Chalupa: Without question. Ukraine is, of course, caught in the middle. It's actually an abused concept, and it's very much driven by ... I wouldn't say driven, but Henry Kissinger, the war criminal, is an advocate, and Henry Kissinger likes to push his chess map-making of the world, his geopolitical vision of Ukraine just being some borderland country that is shared or fought over by the East and the West. Whereas, the Ukrainians themselves caught in the middle are saying, "We just simply want to be a democracy. We want to be a sovereign nation. We are not your pawn." But because, as you go into so perfectly in your book, Ukraine's centuries of colonial occupation by the Kremlin, which includes a horrific genocide, which is one of the worst genocides of the 20th century. Ukraine, according to the historian, Timothy Snyder, suffered the worst under Stalin, the mass murderer Stalin.

Ukraine had it the worst under Stalin. The fact that the country even exists is a miracle. For Ukrainians themselves, they just want to be a sovereign nation and that's it. The US and Europe, with its promises of democracy and relative economic stability and so forth and the way Ukrainian kids growing up with the internet see kids their age in London and New York and LA live, they want that lifestyle. They want to have that, live free of corruption. Corruption being a homegrown issue in Ukraine that the Kremlin very much leverages to keep Ukraine in its orbit. I just wanted to point that out because at the center of this, of your book, is Ukraine, but at the same time, you do have these rotten actors coming in and treating Ukraine very much like a pawn for its own gain, like Putin has been doing.

Andy Greenberg: And like Trump, obviously continues to do with this Zelensky call.

Andrea Chalupa: The quid pro quo, yeah.

Andy Greenberg: Ukraine has remained this pawn of the West and of Russia. When I say that, I don't mean to belittle the experience of Ukrainians. That is how Ukraine has been treated. It has been treated as a little Russia, as a borderlands, as something for the Nazis and Soviets to fight over for its history. But of course, Ukrainians want to shift the border east and be part of the West. I think that that's clear. But nonetheless, sadly, Ukraine has this history of being a borderlands, of being caught between different warring powers. The theme of the book in part is that Ukraine has been this victim of its geography, but we now live in a world where cyberwar does not respect borders. This is a war that takes place in a different geography, without borders, and if we allow a conflict to unfold in Ukraine on this borderlands, then we will all share its fate.

Andrea Chalupa: No, I think you said it perfectly because the moat of America's oceans can no longer protect us. We always had to go over there to fight the fascists. Now the fascists can come into us through cyberwarfare.

Andy Greenberg: Right. For generations, we've allowed conflicts to play out in places all around the world like Ukraine and treated them as these faraway foreign problems, but in a world without borders, in a new realm with a different geography, the internet, where cyberwar is a possibility, then we all live on this borderlands. In this borderless world, we are all on the borderlands and we will all become subject to the same kind of victimization. That's the lesson and the warning of this book.

Andrea Chalupa: Yes, without question, which makes *Sandworm* essential reading. Now let's talk about the passage I had you read, June 2017, this horrific unleashing of an attack that spread around the world. June 2017 is an interesting date. That month of June, 2017, I'll never forget that month. In June 2017, I remember making a trip to Kyiv for my film cause we were going to shoot *Mr. Jones* there, and being nervous about it because harassment was picking up at my sister's home in Washington DC. As you know, my sister worked for many years for the DNC, and she essentially raised the alarm on Paul Manafort, and she was trying to warn journalists as well as people at the DNC that Paul Manafort was here, that meant that the Kremlin was here, and of course, she was dismissed. People thought that was really far-fetched.

Turns out she was right. As a result of being the first voice to really expose Paul Manafort in the 2016 election, she has suffered intense harassment by American Corporate Media and the Kremlin's propaganda machine, and it goes all the way up to the President of the United States trying to invent nonsense on her.

Andy Greenberg: I try not to delve into these conspiracy theories, but if I understand correctly, it sounds very similar to what's happened to CrowdStrike, for instance, is an American company co-founded by a Russian immigrant who were some of the first to point to Russia as being behind the DNC hack. Now, somehow that has become this bizarre fever dream where CrowdStrike is a Ukrainian company and they are fabricating Russia's involvement in this. I feel like I get dumber the more I read about these theories. So I try not to, but it sounds like something similar has maybe happened to your sister.

Andrea Chalupa: Yeah, exactly without question. It's basically, the Kremlin and Trump's White House are trying to harass and get into trouble legally and ensnare the people that caught their crime. But in June 2017, the harassment at her home started to pick up again, and we thought that was really odd. We're like, "Why are they coming back around again?" Because during the 2016 election when she was speaking out about Paul Manafort, there was an attempted break in on her home. They've broken in to her car twice and trashed the insides. Her phone was hacked, her computer was hacked and so forth. Those activities picked up again in June 2017. So, I was nervous about having to go to Kyiv about this time, but I went anyway. At the same time, you had a lot of these Republicans on cable news suddenly changing their tune and saying that collusion is not a crime.

"Collusion is not a crime." And we're like, "Why are they all suddenly saying that?" Lo and behold, it turns out that, at that same time, the New York Times was working on its series of bombshells on the fact that Donald Jr., they're about to come out and blow the lid on this big story, this smoking canon that Don Jr., in June 2016, a year earlier, was taking meetings with lobbyists and lawyers linked to the Kremlin, along with Paul Mantafort and Jared Kushner, the President's son-in-law. This was a huge, huge, massive story. In very, very early July, like July 8th or something like this, the story broke and everyone thought, okay, they finally have them, here's the smoking canon, Don Jr. is going down, Jared's going down, they're finally going to get Paul Manafort.

Instead, what happens shortly thereafter is, Don Jr. breaks his silence on Twitter by posting some tweet about how my sister and Ukraine hacked the 2016 election. My sister becomes a huge story, a huge story in the mainstream media. And people are suddenly digging into her to see if there's anything there, and it turns out, of course, there's not. But what was interesting was we basically, looking back, saw that they were coming around her house, harassing her again to freak her out so she'd be in a weaker position when they finally struck to try to deflect from the Don Jr. bombshell in the New York Times.

I think the timing of this big Russian cyber attack in June 2017, it's very difficult for me not to think, well, were the Russians also in on this and trying to wield a well used intimidation tactic against us? To be like, look, if you really go after the president and his family who we need in power, because they're our allies, we are going to inflict damage on you. Do you think that there's any there, there in terms of that being connected?

Andy Greenberg: I am so sorry to hear your sister went through that. I wasn't aware of most of that, but I think that it's more a testament to just how prolific Russia's hackers may be. I don't know if they were involved directly in your sister's ... the compromise of her computer or phone or anything, but it certainly fits with, specifically the more like the activity of this other GRU hacking team. EBT 28 or FancyBear, and I'm just wildly throwing this out. I have no idea. I shouldn't say that I believe that they're ... I don't believe that they're responsible. I'd have to see evidence.

Andrea Chalupa: Of course.

Andy Greenberg: Just within the GRU, there are espionage teams, hacking and leaking teams and then there's Sandworm, which to me has always seemed like a sabotage disruption team. That's just within the GRU. There's also of course the FSP and the SVR. They are all even competing with one another to be the most aggressive to impress their bosses with greater and greater acts of aggression and just rampant spying and sabotage influence operations. This was happening physically too, of course, there's the ongoing war in the East. Then on June 27th, 2017, the very first thing that happened that day was a bombing, a car bombing of a Ukrainian general. He was murdered in the middle of Kyiv.

That was, in some ways, the first shot fired that day and even that bombing hit civilians who are just walking on the street next to his car. I describe that in the book as the first collateral damage of the day that would see massive digital collateral damage when NotPetya hit just minutes later. What I mean to say is that Russia's intelligence services seem to have a culture of just constantly trying to outdo themselves to do everything that they have and their capabilities to their enemies and especially to Ukraine.

Andrea Chalupa: Yeah, but do you think that this capability, having this highly destructive and determined Sandworm team of hackers, do you think that the Kremlin would wield that or has wielded that as essentially an intimidation tool against us here in the US in regards to trying to avoid any accountability? Because they did that against Ukraine. Hacking the election, as part of its invasion, it's punishment of Ukraine for overthrowing Yanukovych.

Andy Greenberg: Sandworm, to me, seems to be this kind of collection of motives, these disruptive acts of massive sabotage. They do send a message to the West. They say, "We have this ability, if you mess with us, we can turn off your power, we can unleash destructive worms in America." That does box in what I think the US is willing to do in Syria, in Ukraine, for instance, when we know that that capability is in Russian hands. But there's also almost terroristic effect of these attacks. They are their own sort of influence operation. They make Ukrainians scared. They make Ukrainians lose confidence in their own governments. They try to make Ukraine look like a failed State. That is, I think part of their intention.

I think that if you ... it's hard to get inside the mind of a GRU agent, but from what I can tell, talking to Russian analysts and reading every memoir I could of a GRU defector, there seems to also just be a kind of massive machismo within this agency that you just do every aggressive thing you can to impress your boss. You win points for ... not for being risk averse, for considering the consequences of your actions, but for just doing it, for doing the thing that you figured out how to do. I think maybe the best example of this is the GRU attack that is in the third act of my book on the Olympics in 2018.

This was an attack where the GRU tried to frame North Korea for their own disruptive cyber attacks that almost took down the entire IT backend of the 2018 Winter Olympics and they didn't want to send any message with that. They were trying to make it look like it was North Korea attacking South Korea, but internally they must have felt some sort of sense of petty revenge that we've been banned from the Olympics for doping. So we're just going to do this to feel good for ourselves to make our bosses happy that if we can't enjoy the Olympics then no one will. I don't think we can rule out that kind of pettiness as a motivation as well.

Andrea Chalupa: It's very chauvinistic as well. If you look at social issues in Russia itself with domestic violence and violence among men and just alcohol abuse and so forth, it's very much seeped. Unfortunately, is a problem for the Russian people themselves. They're battling with the biggest dog in the fight wins, might is right mentality, even locally. These hipster kids that go out protesting against corruption and so forth, they're getting sadistically beaten by riot cops because it is unfortunately, systemic in that culture right now under Putin, and like you said, it's promoted under Putin that might makes right.

There is obviously an opposition towards this and there are a lot of brave Russian men and women that are trying to confront this, and very much risk in their lives to do so and their family's lives just by showing up at a protest themselves. But to your point, we have to also be anthropological about this and say that Putinism, Putin's Kremlin, is encouraging this might is right and that sometimes it is just a matter of violence for the sake of violence and destruction for the sake of destruction to really prove a point and to intimidate and to bully people into submission.

Andy Greenberg: I think you're right and I try to be careful. I think you're being careful too about not trying to cast some stereotype against the Russian people or Russia as a whole or to be Russophobic. I think Putinism them is a great way of describing it, and I think that that culture of Putinism, that kind of hyper aggressive machismo is endemic in the GRU specifically.

Andrea Chalupa: Exactly. It's toxic masculinity. As we're always saying on this show, white supremacy, toxic masculinity, they're some of the greatest threats right now the world is facing, and Putin embodies that with his shirtless photos. He bikes around with this Far Right biker gang thinking he's very tough. He tries to essentially emasculate men, especially that are on the front lines of trying to say there is an alternative to Putin in Russia. There is another Russia. There is another way. Obviously this is the larger conversation. Boris Nemtsov being wonderfully charismatic, and it's hard not to point out, a handsome figure like a tall strapping handsome Russian man being very charismatic and brave and saying, "We're going to do a March. Russia invaded Ukraine. Crimea belongs to Ukraine."

Boris Nemtsov had to die. He had to be killed in Putin's world because he represented such a threat. He needed to be brought down as part of that sort of might is right, violence is deserved sort of way. So, when he was killed, a lot of the conversations sprung up, well, the order didn't come from Putin directly. Putin, at least, created the environment for Boris Nemtsov to be murdered.

Andy Greenberg: I'm not inside the Kremlin's hierarchy enough to know, did Putin order of these things? I have a feeling that he didn't, probably as you say, these were acts that the GRU, with its own full independence, may have carried out, just to impress generals, to impress Putin, of course. I have had to try to piece together this psychological profile because I couldn't interview GRU agents, despite getting as close as standing outside their building in Moscow. You can't knock on the door. You can't ask for an interview with GRU unit 74455. That's not going to work. I did my best to speak to people who have tracked the GRU for years, to read the books of the few defectors who have told their stories and to try to fit that in with this jigsaw puzzle of their actions that we can see forensically around the world.

Andrea Chalupa: So, how does the Kremlin work with hackers? Do they have the hackers on staff at the FSB that are employees and they see them as, I'm guessing military officers essentially? Or do they also work with some freewheeling groups out there? What's sort of the overall ...?

Andy Greenberg: I tried to figure this out. There's this problem with cyber attacks, of course, it's called the attribution problem. How do you figure out who was behind them? It's far more difficult, and sometimes impossible to actually get definitively to a person's identity as the culprit. But we have been able to identify some of the GRU agents. Thanks, in part, to Robert Mueller's indictments in 2018 of 12 of those agents involved in election meddling. Some of them have also been tied to these disruptive attacks as well. I also spoke to GRU experts in the US and Britain and Russia who gave me some sense of how the GRU functions compared to the FSB, for instance.

Part of the story I heard is that the FSB has a history of recruiting sometimes, involuntarily, cyber criminals to act on their behalf. That they kind of muscle them into doing the FSB's bidding with a threat of law enforcement. But the GRU, far more often at least, seems to train and build its own teams internally like a military agency would, and that these hackers are wearing uniforms and showing up for work inside of a military facility in many cases. When we saw these 12 hackers, many of whom were literally in uniform in the wanted posters that the Department of Justice has released, that was partly confirmed I think.

Andrea Chalupa: The really interesting thing is there have been some headline grabbing stories of Russian hackers just committing cyber crimes against American banks and big tech companies like LinkedIn and so forth. It's really interesting that you have these well-known capabilities of Russian hackers committing crimes just to enrich themselves and their own fun and games. Then the Kremlin trying to, I'm sure, tracking these guys as talent pools, wouldn't you imagine?

Andy Greenberg: That's, I think, historically been how a lot of the Russian intelligence agencies' recruitment has worked. I think that Sandworm is distinct from that in a way because, from what I could tell, it seems like these are the Russian government's homegrown hackers that they are trained, hence groomed, from within. They are military hackers. Maybe they have some sort of cyber criminal background that allows them to develop some of their talents, but they are not that model that we've heard of elsewhere where a cyber criminal hacker is caught in the act and then brought under the wing of the FSB.

Andrea Chalupa: There's an interesting story, I don't know if you've been following it, where an Israeli-American woman who was traveling on vacation, taking a connecting flight through Moscow to try to get back home to Israel and she was stopped in the Moscow airport. She's now in prison because apparently, allegedly they found some weed, some marijuana on her that she was traveling with and they bumped up her charges to essentially saying that she's a drug smuggler. Israel wants her back and there's been a lot of interest in her case that's fortunately building because the whole story just stinks. Essentially, Israel right now is keeping a Russian hacker and the Kremlin now wants to give back this poor Israeli-American woman they've arrested and are holding in prison for so-called drug smuggling, they want their hacker back out of Israel in exchange.

Russian authorities would go to the point of arresting and holding a woman, vacationer, just to try to get back a Russian who's being held in Israel because he's wanted by the US for suspected cyber crimes. That's pretty brazen, wouldn't you say? I don't know if you followed this story at all, but it's sort of that, the fact that Russian authorities are doing this to a close ally under Netanyahu's government, certainly Israel, by holding one of their citizens hostage in a hostage situation and hoping to swap her this holiday maker for an accused Russian hacker being held in Israel because of US charges. That's the length they seem to be going to try to protect their talent pool or potential talent pool or ...

Andy Greenberg: It's remarkable that there have been several rounds of indictments now of Russian hackers for election meddling, and then in fact, for some of the Olympic related attack, not the actual disruption ...

Andrea Chalupa: The winter 2018 South Korea, Olympic attacks.

Andy Greenberg: There was no indictment or even public statement about that attack, which I think is another failure of this digital diplomacy that we should be doing. But there was in fact, an indictment of Russian hackers who are attacking anti-doping agencies and hacking and leaking their emails. This is another kind of Russian hacker obsession. It's like Ukraine and NATO and the Olympics weirdly, is another one on that list.

Andrea Chalupa: Well, because they don't like accountability. They don't like to get called out. So, the Olympics was forced to do that because the doping scandal was so systemic in Russia with the Russian teams. It seems very reactionary to being called out.

Andy Greenberg: Certainly, and I think it does give us one more hint of the mentality of the tasking of these hackers that when there is a slight to Russia's national pride, that is a moment when they can be mobilized. In all of these indictments, there's yet to be, as far as I know, a single one of these GRU hackers who is actually imprisoned or actually faces justice. When that happens, and I'm not that familiar with this Israeli case, I can imagine that Russia has a lot of resources to put into freeing their person because it happens so rarely. These hackers don't seem to travel abroad. They don't go on vacation in Thailand and get arrested as some other foreign hackers do. They seem to have learned those lessons.

Andrea Chalupa: Right, because there was one Russian hacker who went to Prague on vacation. "A man identified as a Russian hacker, suspected of pursuing targets in US has been arrested in Czech Republic." Yeah. That is from the New York Times. Yeah. "The social media company, LinkedIn said it believed it had been a victim in the case." That was the LinkedIn hack. This kid went abroad to Prague and they swooped in and got him there. To be a Russian hacker, essentially, you got to really enjoy a vacation at Belarus. You're kind of limited.

Andy Greenberg: Or Crimea.

Andrea Chalupa: Or Crimea now, unfortunately, but hopefully not for long. We should talk about the US and our capabilities because right in the weeks after the 2016 election, I was chatting with an American who owns a private firm where he employs hackers. He explained to me the complexity, the sensitivity of recruiting hackers good enough to work at his firm where he gets paid a lot of money to break into hospitals and major corporations to look for vulnerabilities and advise on how to fix it. So, he was telling me that the US remains the best in the world in terms of our cyber capabilities and that attacks from Iran and Russia happen pretty much every second of every day and we're constantly stopping them. We're constantly doing our own attacks that people never even hear about.

Andy Greenberg: I think he's right, at least, in saying that American government hackers are the most sophisticated, the NSA and Cyber Command, which is the associated part of the Pentagon that carries out the actual offensive, our version of Sandworm. Although, that may be like ... that's not really the right way to say it because Cyber Command, when they do these disruptive attacks, and this is the caveat to saying that the most sophisticated, is that they're extremely restrained legally and I think even ethically in what they do. They sabotage activities of cyber command. When they destroy a network that belongs to an enemy, they seem to be fairly well targeted. They don't cause blackouts, they don't affect hundreds of thousands of people. They don't unleash worms that spread from one country to another. They take out, for instance, the network of the internet research agency or an Iranian espionage team.

They seem like they are pretty targeted, and even Stuxnet, as controversial as it may be, it was an extremely targeted attack that was designed to do one very specific thing, which was to destroy these enrichment centrifuges. Whereas, when Russia does the same thing, and Russia probably is nearly as sophisticated in some ways as American government hackers, but they are willing to use every tool in their arsenal in a way that American hackers are not. There's no question that the NSA could be causing blackouts, could unleash terrible worms across the internet. In fact, part of the story of Sandworm is how some of the NSA's hacking tools were stolen and used by North Korean and then Sandworm Russian hackers to inflict elements of their terrible damage.

But, aside from those occasional disastrous leaks of NSA tools, for the most part, the NSA is very, very careful and restrained, and mostly just does vast espionage and nothing more aggressive than that. Whereas, Russia and then less sophisticated teams of hackers and countries like Iran or North Korea just do whatever they can to disrupt the global order in many because that is their goal. They don't ...

Andrea Chalupa: It's terrorism. It's terrorism.

Andy Greenberg: Hackers in countries like Iran and North Korea and Russia, they have a kind of insurgent mentality. I think they want to blow things up in part because that is how you destabilize the global order and put yourself in a better position. Whereas, the US, and even China, they use their cyber capabilities very strategically just to advance their own interests, and in a way, that is often pretty restrained and limited. Even in China's case, it's really just espionage for the most part. Of course, they do terrible things to their own citizens and they spy on Tibetans and Wiggers. The results of that are terrible oppression, but internationally trying to just spy is, for the most part. They don't destroy things. They don't unleash worms, but we've seen that from Iran, North Korea, and Russia, probably to the greatest degree of all.

Andrea Chalupa: Right, which is why we're talking so much about the Russians versus the Chinese. Kremlin aggression has pretty much dominated a lot of the media discourse since Trump came to power. China's authoritarianism, what they're doing is, I would even say to their own people, you have gulags being built in China. It's horrific. I think it's important to confront what Putin is doing to, not only globally, but also to the Russian people. I think it's important to have that discussion so we don't forget and we follow that story because they're determined actors, but also we cannot forget China. It's horrific. The authoritarianism.

Andy Greenberg: The Chinese people are another victim of the White House's isolationism and it is tragic. But if you take this very callous approach of saying, "Well, that is their problem," that may be true in China's case. It is an ethical calamity, but that kind of surveillance is largely limited to China. Although, it's spreading. I think, well, I don't know. I don't want to say that. This isn't my topic. I'm getting farther away but I ...

Andrea Chalupa: I think to the larger point is that the world now is finally being forced to catch up. That regional aggression is no longer contained in just that region, because before, in the lead up to World War II, for instance, you could have the US Congress debating ... American politicians debating whether to help out the Europeans with the rise of Hitler and the horrible things that Hitler was doing, and they had the luxury of debating that and the time to debate that. Whereas today, anytime you have a really aggressive determined actor like Putin, you don't have much time to debate what to do about him because he has the weapons now to spread his aggression well within your borders, and that's essentially what is at heart here.

Andy Greenberg: Let me try to restate what I said. Yeah. You can take this very callous approach to treat what China is doing to its citizens as a Chinese problem, which is sadly I think true to some degree. In some other ways, China's surveillance techniques are spreading to the rest of the world, and China is growing its Capitalist empire, but I think in a much more direct way, what Russia is doing, you can also treat it with this isolationist lens, but that is a bigger mistake because Russia is far more willing to reach out through the internet in some cases to attack global targets in the West or in Korea. We saw Russia attack the 2018 Olympic games with very intentional and targeted cyber attack that took down the entire IT network of the games at the moment that the opening ceremony started.

That is something that I think has not gotten enough attention and shows the willingness of Russia to reach into these global events. An event where heads of state from around the world and these foreign dignitaries were present and just try to just mess everything up for its own weird petty pride. I think that you can be isolationists, and in some cases, that maybe is self-interested in this extremely Trumpian selfish way. But in other cases, it's just a huge mistake, no matter what you're ... even if you're just selfish, that the Russian government, the GRU does pose a global threat that needs to be countered.

Andrea Chalupa: What do we do about it? What do you know is being done about it?

Andy Greenberg: Well, I don't want to sound like a hawk because I don't think that ... I'm not asking for some sort of neoliberal conservative war against Russia as a result. I'm talking about diplomacy, I'm talking about the kinds of tools that we have used, in some cases, often too late or in a weak way, but indictments of hackers that do limit their personal lives, sanctions that punish the Russian government. I think ...

Andrea Chalupa: Banks not tanks is what you're saying. Basically holding a kleptocracy accountable.

Andy Greenberg: Exactly. Then, the easiest thing of all is just to talk about this publicly. We saw Obama give a speech about North Korea hacking Sony Pictures and yet nothing about Russians hacking Ukraine and causing the first ever blackout. Why don't we see more White House statements about these unacceptable cyber attacks saying this is a red line? The arena of cyber warfare is one where the red lines are still being drawn. If you don't call out unacceptable attacks, then you essentially are telling the adversary, "Well, you haven't crossed the red line yet. Keep trying." And that's what they've done.

Andrea Chalupa: Right. So sunlight is the best medicine.

Andy Greenberg: I think more than sunlight even. Sunlight is like in the media, like me shining a light on this stuff. But I'm talking about official rebuke, hence acts of rulemaking, setting boundaries. Ultimately, I think we do need something like a Geneva Convention, what Brad Smith and Microsoft has called for, a Geneva Convention for the internet, for cyberwar. Another person I spoke to in the book is Josh Corman who spoke about No Fly Zones around certain civilian critical infrastructure, digital No Fly Zones like, you can do what you like in a cyberwar, but if you touch a hospital, if you touch a power grid, then you're going to end up in the Hague because that's a war crime, and I think that that's a powerful idea as well.

Andrea Chalupa: Our discussion continues and you can get access to that by sending up on our Patreon, at the truth teller level or higher.

Sarah Kendzior: We want to encourage our listeners to donate to RAICES, a Texas based nonprofit agency that provides free and low cost legal services to underserved immigrant children, families and refugees. They're helping with the crisis facing migrant families at the Texas border and need your support.

Andrea Chalupa: We also encourage you to donate to help critically endangered orangutans already under pressure from the Palm Oil industry. Donate to the orangutan project at theorangutanproject.org. Gaslit Nation is produced by Sarah Kendzior and Andrea Chalupa. If you like what we do, leave us a review on iTunes. It helps us reach more listeners, and check out our Patreon, it keeps us going.

Sarah Kendzior: Our production managers are Nicholas Torres and Karlyn Daigle. Our episodes are edited by Nicholas Torres and our Patreon exclusive content is edited by Karlyn Daigle.

Andrea Chalupa: Original music in Gaslit Nation, produced by David Whitehead, Martin Disenburg, Martin Visenberg, Nick Farr, Damian Arriaga and Karlyn Daigle.

Sarah Kendzior: Our logo design was donated to us by Hamish Smith of the New York based firm, Order. Thank you so much Hamish.