3 Takeaways Podcast Transcript
Lynn Thoman
(https://www.3takeaways.com/)

Ep. 159: A Top National Security Expert Explores The Critical Role Cybersecurity Plays In America's Security

This transcript was auto-generated. Please forgive any errors.

INTRO male voice: Welcome to the 3 Takeaways podcast, which features short, memorable conversations with the world's best thinkers, business leaders, writers, politicians, scientists, and other newsmakers. Each episode ends with the three key takeaways that person has learned over their lives and their careers. And now your host and board member of schools at Harvard, Princeton and Columbia, Lynn Thoman.

Lynn Thoman: Hi everyone, it's Lynn Thoman. Welcome to another 3 Takeaways episode. Today I'm excited to be with Anne Neuberger. Anne is the Deputy National Security Advisor for Cyber and Emerging Technologies in the Biden administration. Prior to this role, Anne spent over a decade at the National Security Agency, as Director of Cybersecurity, as Assistant Deputy Director of Operations, and as the Agency's first Chief Risk Officer. I'm excited to find out how Anne sees cyber, artificial intelligence and other threats. Welcome, Anne, and thanks so much for joining 3 Takeaways today.

Anne Neuberger: Thank you, Lynn. It's wonderful to be here with you.

LT: Thank you, Anne, for all you do. Your job is so challenging.

AN: I feel very fortunate to have the opportunity to work on these, you are right, very challenging issues.

LT: During the Obama administration, reportedly the Russians hacked the White House, the State Department, and the Joint Chiefs of Staff, and the British warned us that Russian military intelligence was inside the Democratic National Committee. What is the current cyber threat landscape and what lessons have we learned?

AN: When we think about cyber threats, I look at them in two categories. First, there are significant criminal cyber-attacks driven by financial reasons. We see ransomware attacks in the United States, around the world, affecting manufacturing companies, affecting hospitals, schools, and that's one set of work. And because criminals cross borders, this is a transnational threat, we've driven an international collaboration, we kicked it off two years ago, in which we have 40 countries working together on fighting this threat across disrupting the individuals who often live in countries that are not responsive to law enforcement, disrupting criminal illicit use of cryptocurrency, which is how these entities work to force ransom payments. And finally, working on resilience, what's needed to lock down and defend such systems. That's one set of work and one set of transnational cyber threats. The second is countries, a number of countries have very capable, sophisticated cyber programs, both for espionage, even more concerning for disruption purposes.

AN: When Russia invaded Ukraine, on the eve of the invasion, Russia conducted a cyber attempt

against the satellite communications company, which provided services to Ukraine's military communication services enabling them to communicate, which also served a whole set of critical infrastructure in Europe, from German windmills to other entities, to a bunch of consumers across Europe. That disrupted those services. And that gives a picture of the second set of threats we look at, which are nation state programs that work to disrupt government or critical services in countries as part of their broader foreign policy goals. To your question of what we've learned, first, it's fundamentally a transnational threat. Second, to take on criminals, ensure that there are laws that can bring them to justice that are enforced, and then as an international community, we're working to put in place the international norms to make this activity unacceptable is the final piece of really tackling this.

LT: Anne, can you talk more about the lessons that we've learned from Ukraine?

AN: Absolutely Lynn. Really three Ps, as we say, preparation, partnership with the private sector and international cooperation. On the first, preparation, in cybersecurity, the work the country does to lock down doors and windows, to lock down critical services, to ensure there are backups for critical national data is key. In Ukraine's case, in the run up to the war, once we were working to share intelligence and ensure that as many entities around the world as needed to know, including Ukraine, knew about Russia's preparation for the invasion. Ukraine accelerated their work to disconnect from the Russian electricity grid, connect to the European grid, and to move their data, to change their laws to enable them to move their data to the cloud, e.g., to have a backup that was independent of infrastructure in the country. That preparatory work was critical to Ukraine's ability to survive the Russian cyber-attacks that began with the invasion and have continued unabated throughout that period since then.

AN: Second, partnership with the private sector. We saw American and European companies surge to support deploying cybersecurity defenses, providing free services. The capabilities the private sector brings from a cybersecurity perspective, not only for Ukraine, but by having the capabilities in place to detect Russian offensive cyber activities and push out those defenses globally, those companies really kept the world safer from Russian cyber-attacks. And finally, international cooperation. You've certainly seen both the cooperation in terms of sharing, spread information between countries. We also work together to ensure that our responses are in unison. Following, as I mentioned earlier, Russia's cyber-attack against the satellite company, which provided services to Ukraine, we worked with our European Union partners to call out that activity and say it was unacceptable as part of that work, among an international set of partners, to define cyber norms.

LT: How do you see artificial intelligence changing war?

AN: Technology has long shaped war, has long shaped foreign policy. Countries, which adapted technology and attracted skilled labor drove productivity, drove economic growth. And militaries that adapted technologies, from advanced platforms to robots for hazardous missions to drones for precision intelligence, were more able to project power on the world stage. Certainly, as we look at AI as the future of war, the potential misuse of these technologies heightens concerns about warfare in the digital age, the erosion of traditional deterrence, the ethical implications of their deployments.

LT: It seems very challenging because AI is so much faster than humans and makes decisions that humans might not make. Does that mean that a country that has humans in the loop will be at a disadvantage if they're attacked by AI that is operating at superhuman speed?

AN: It's a good question. I believe a country's global leadership is a combination of its values and then how it can project power. And as a country in which our values, or what has always been a part of American leadership, that value to say we must ensure a human in the loop arm critical uses of AI is something that we're committed to as we also look to ensure, how does AI help ensure we can project power to keep the United States safe, to keep our allies and partners safe, to keep the world safe. But it's certainly that sense of how countries values translate into those decisions is a key challenge we will be facing, and we will need to work together to create international norms that bring our best selves, our best values, into these decisions at all times.

LT: So far, we've talked about cyber and AI. What other threats do you see?

AN: Certainly, it's related to AI, but the disinformation threat, the way that deepfakes can bring additional risks. Whether as we're already seeing deepfakes threatening women from a pornographic perspective in terms of creating fake pornographic images all the way through to fake video. Think about the Zimmerman letter, a fake video that pretends to have a political leader instructing particular military operations, and having a way to detect that that's fake and respond to that rapidly. That's certainly one key area. Climate change is a whole topic of its own. Looking at the risks of climate change, food generation, vulnerable population, and how we build on the global cooperation with the sense of urgency needed to counter that is certainly a key area. It's very much a concern as well. And then the health of the international order. Russia's invasion of the Ukraine and ensuring that we maintain the global partnership to say there is international order, there are rules that we must work together to maintain for national, international safety and security.

LT: Many of the potential targets of both cyber and AI are in private hands, such as financial firms, electric companies, internet companies, water companies, and hospitals. But now we also have so many internet-connected devices in our personal lives, from our phones to our computers, our cars, our Alexa devices, and other devices. And no matter how much better we get at defense, there are just so many more targets. Can we protect ourselves in this interconnected world?

AN: We absolutely must, and we've taken two approaches to that. I would say that first is an effort that we launched that brought together the private sector, the government and the idea that we must work together to keep consumers safe. And that is the Cyber Trust Mark program, which was launched that essentially says, individuals around the world are bringing all kinds of internet-connected devices into our homes, into our schools, into our businesses. And American consumers, when they're shopping for a device want to know that device is secure. They don't need to know every detail, what makes it secure, but they want to look much as we look for nutrition labels as we shop for food, or we look for an energy star label to know that a device is energy efficient, and then when we plug it into the wall, it won't explode. We need the same for cyber.

AN: The program we launched led by the Federal Communications Commission, with a number of leading companies from Google to Amazon to LG agreed to participate in, has a standard for internet-connected devices. If companies meet that standard, they can put on the US government Cyber Trust Mark logo, which we believe will give consumers that sense of trust and confidence that this device meets US government defined cybersecurity standards. We hope that by the end of 2024, Christmas of 2024, there will be devices on shelves, shopping online that Americans can look for this mark. I'll note that that's also something we're working globally with countries around the world because that's very much a sheer interest.

AN: The second part of that is as a country, we need to know that the critical services we rely on every day, the electricity, financial firms, water, healthcare, meets cybersecurity standards. As I say, they've locked their digital doors, they've locked their digital windows, and they've censored it to rapidly find an intruder who breaks in. And as a result, following the Colonial pipeline cyber-attack in 2021, the White House has been putting in place minimum cybersecurity requirements for various critical service sectors, from pipelines to railways to water systems, so that we can have that confidence that companies operating those critical services have put in those basic safety and security controls to keep them safe in cyberspace.

LT: Anne, the NSA is often portrayed as an insular culture. And yet you joined mid-career and proceeded to lead complex, large organizations with global missions. Was that unusual? And what have you learned about breaking into insular cultures?

AN: It was unusual and it was certainly difficult. Cultures are sources of strength. Cultures can be sources of weakness and certainly very proud cultures, cultures that have storied pasts are very much a combination of both because they can often be, as you know, difficult for people to contribute, to break in. At the National Security Agency there's a very proud culture of people coming in straight out of college and working there for 20, 30, 40 years of a career. I would meet people who are getting their 50-year government service pin. There's incredible strength in that. There's also incredible strength in a culture that can both allow people to leave and potentially come back and accept people who have not had 15, 20 years of experience in different arenas and contribute and come in and contribute that history.

AN: I learned three things. One, in such cultures, one needs to set aside what you've done before and really just communicate respect and eagerness to learn about the culture and an eagerness to contribute because that sense of mission often drives these cultures and talking about your desire to contribute to that is key. I think the second thing was being prepared to take the job no one wants, because those are ways one can prove both one's desire to contribute and also that the different background perhaps gives you a way to contribute in that way. And then finally that it's all about people and forming relationships and building relationships with people is a good way, asking for their help. Acknowledging that one needs that help, I think is the final lesson I've perhaps learned about how one breaks into and how one enters and contributes in very proud, but perhaps insular cultures.

LT: Women often grapple with how much they can bring their whole selves to work. Do you have a perspective on that particularly in a male dominated national security field?

AN: Yes. A number of years ago when I was serving in the intelligence community, we had an internal blog in the intelligence community. And I wrote a blog and I talked about how in my family background on Hanukkah the tradition is to light a menorah at a window, to talk about the miracle that just believe happened over the holiday. The small vanquishing the very strong, the fight to pursue and live one's faith. And growing up, my father, my parents would light our family Menorah inside the house, not at a window. And I had never really, I'd never really thought about it. And when I got married and we were lighting our family Menorah, and we put it on the windowsill as is tradition. And I had realized suddenly that as a child we'd never done that. At some point I was talking with my father and I said, "Why didn't we follow custom?"

AN: And he kind of looked at me and said, "Growing up in Budapest, a menorah on a window would've meant a rock through the window. And when I came to America, I just, I was afraid." And I thought to myself that what a privilege it is, that didn't even occur to me to be afraid to light our Menorah, that my children didn't even think twice about it. And I wrote a blog post for that internal kind of community talking about my gratitude of the work each person there did to keep this country safe, to project our values, to work around the world so that we could try to be a force for good in various conflicts around the world as well. And before I hit publish, knowing it was going to thousands of people, I paused and said, "Do I want to show that vulnerability?" because particularly as a woman, it wasn't easy.

AN: I faced harassment as a woman in the national security community. I faced double standards as many women. And then I said, you know, being a woman cuts both ways because we can use that sometimes extra sense of sensitivity to people to show that that helps people bring their whole selves to work. And I pressed publish and I paused, it was a hard thing to do. And then over the ensuing days, weeks, months, years, I've gotten emails from folks of very diverse backgrounds who talked about how the email made them think about their own background and feel they had the courage to bring that part of themselves to work. That is one part of women grappling with that. And the second part is, just overall, women do sometimes face double standards. And pushing through that, people will often say, "A strong woman is viewed in one way and a strong man is viewed in another." And knowing that one has an obligation to use one's strengths, to use one's talents for good, sometimes means taking those double standards, swallowing and moving on.

LT: Anne, before I ask for the three takeaways you'd like to leave our listeners with today, is there anything else you'd like to mention that you haven't already touched upon?

AN: Lynn, you've been very thorough, so no.

LT: Anne, you've been extraordinarily open! Thank you. What are the three takeaways you'd like to leave the audience with today?

AN First, I'd say America's a country of stories and a dream that from many stories we can have one nation, one message of benevolence and acceptance. In my case, it was a father and grandparents who came here fleeing something and dreaming of something. For other families, it could be a great, great, great, great, great grandparent. But we all have an obligation together to ensure that for families like ours from around the world, families in the US, we preserve that treatment for many generations. The second one, I would say, as we look at new technologies like AI, let's keep one eye on the opportunities to use AI for good. Let's keep one eye on the risks they bring and ensure we're fully using both eyes to drive a path forward. And then finally, security and innovation must go together. We simply can't have one without the other.

LT: Anne thank you, thank you for your service in government and thank you for protecting us all and being a force for good.

AN: Thank you so much Lynn for having me with you today.

OUTRO male voice: If you enjoyed today's episode and would like to receive the show notes or get new fresh weekly episodes, be sure to sign up for our newsletter at https://www.3takeaways.com/ or follow us on Instagram, Twitter, LinkedIn and Facebook. Note

that 3Takeaways.com is with the number 3, 3 is not spelled out. See you soon at 3Takeaways.com (https://www.3takeaways.com/)

This transcript was auto-generated. Please forgive any errors.