Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

7.19.24
10:25 — 11:05 AM MDT
Securing Trust in the Global Digital Economy: Cyber, Fraud, and Emerging Threats
Sir Jeremy Ian Fleming, Former Director, GCHQ
Jon M. Huntsman Jr., Vice-Chair, Mastercard; Former U.S. Ambassador to China and Russia
Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology
Kent Walker, President, Global Affairs, Google
Moderator: **Steve Clemons**, Contributing Editor, National Interest
Session recording:
https://www.youtube.com/watch?v=RLiTm8CUG_s&list=PL7fuyfNu8jfPTKp6PJ2yJugSfxXEDyEqM&index=35

Steve Clemons
Great to have you all here. So Anne, how's your morning been?

Anne Neuberger
That's a great way to start with now, I think the afternoon. So as you would expect, morning started with a 4am call from the Situation Room to highlight the issue that occurred with CrowdStrike. And I think it highlights both the degree to which our economies our national security, are now digital and interconnected in a fundamental way. So where that started was essentially quickly pulling together the US Interagency, first to assess what's the impact on us, government, critical services, second, to assess sector by sector, what's the impact of power in the country, to hospitals in the country, to 911, systems, the National Suicide Hotline, and just we continue to do those calls until we have a good picture now of where we are. Of course, I also put a call into the CEO CrowdStrike to say, how are you Is there anything the US government need to help?

Steve Clemons
And how did George Kurtz sound?

Anne Neuberger
He sounded thoughtful, as one would and like keeping up for a number of hours already. And finally, do you think this is malicious, right? And I think very much at this point we believe that it is an IT related a patch, an issue with that patch. I think they're determining what went on there, but it does highlight the need for us when we are such a digitally connected country and global economy. I also reached out to a number of my counterparts around the world to see if they needed any support from us, or they needed to really share information. I such global interconnected economy, we need to ensure that we have the resilience further to the question

Steve Clemons

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

So take it just a notch further. And I want to go to our other colleagues and say, you know, ask if you were a nefarious player and you wanted to play in this world of hyper connectivity. I mean, I remember we have Zoe Baird in the room. Is, I think Zoe here. Zoe is was at marvel foundation of new america. We began 20 America, 25 years ago, trying to sort of look at what would broadband due to society, and how you develop trust and inclusiveness. How do you get this right? And if you look about it now, coming to an AI world, in a, you know, much more connected world, have we replaced a highly connected world that was supposed to decrease trust, or sorry decreased fear, increased trust, and if we replaced it with a high fear connected world? And is that? Is that where we're at that we can't feel comfortable and safe and secure, even, even if a nefarious player is not behind this incident. I couldn't get into my room last night because they couldn't make a key. I couldn't get on to an Australia TV hit the middle of the night because Australia TV was shut down. So all over the world, this had an impact. So are we now in a high fear connected world, rather than a high trust connected world?

Anne Neuberger
I think we're in a world where we have to work much more rapidly so that individuals can have confidence in the digital systems undermining our lives. What was so interesting about this morning incident is a lot of what we've been doing between governments and strong partnerships between government and private sector has been improving our digital defenses, locking down our digital defenses. The irony of this morning is that a major international cybersecurity company was impacted. So we need to really think about our digital resilience, not just in the systems we run, but in the globally connected security systems, the risks of consolidation, how we deal with that consolidation, and how we ensure that if an incident does occur, it can be contained and we can recover quickly. So there's work to be done to build that resilience. Because frankly, as you mentioned, in a physical world, impact could be contained far more narrowly, both in between impact as well as on the geography of the battlefield. In a digital world, because of that connectivity and the speed we need resilience to be at the same speed.

Steve Clemons
So Jeremy Fleming, not just because we have a British accent, but I know you were one of the great spymasters of the world, and so with homage to Austin Powers, if there was a Dr Evil instigating an incident like this, that maybe an accident, maybe not, but it definitely exposes something when you see something like this. I'm interested in the kind of geopolitical and even the non state actors that are out there trying to trigger a meltdown in modern, connected societies that want to be safe and secure and grow. How do you look at the bad, you know, the evil players out there?

Sir Jeremy Ian Fleming
Yeah, I think that's the first time I've had Austin Powers written a question, and thanks for bringing up my middle name. I'm going to work with the organizers, because I think I'm the only one on the program that has my middle name in it. It was obviously a sick joke by my parents. And I'm also reminded back here in Aspen, the first time that I really came across American industry and high tech was as part of the market Foundation. And coming here and finding that

the way in which America is working, the way in which technology is going and also starting to understand some of these resilience questions. I think resiliency is as American wasn't it, but resilience questions, this is not something that's new, but it has been accelerated by technology and by our dependence, and by the interconnectivity that and Anne and has out outlined there. But is there a Doctor Evil out there? Well, I'm not in that way, someone petting a small white cat, but there are literally 1000s of people that aren't state actors, that are benefiting enormously from criminality in these sorts of systems, and from, if you like, the lack of trust and confidence that we have in these systems. And in many ways, I worry about that a lot more than a nefarious state actor. I mean, of course, I worry about that, and some of the experience that we've seen here in America, some of the way in which state actors have gone after critical national infrastructure here, which is only, can only be seen as pre positioning. We must worry about that. But it's criminality, and the way that that under undermines trust in the whole system. Now, the crime that you're most likely to suffer in the UK, I think it's the same. It's now a cyber crime, it's a fraud crime, and the reality is that our systems are very poor at dealing with that. They're very poor at following up on it, and any imposing any sort of cost on the actors around all of that. So, so yes, think about a, you know, an Austin Powers, Dr Evil. But actually, just think about the criminality that is underpinning a lot of the ways in which our trust is being undermined.

Steve Clemons
You know, just just one quick item, though, you know, if you do have state banks, think of China. You think of North Korea, which is which has sponsored attacks. We know, the famous Sony attack long ago, or Belarus Iran, others that are out there. I think one of the questions in this space, and Jane Harman struggled with this when she was President Wilson centers out there, is the question of, how do you set up deterrence? Do we have as much malware in their electric grid as they have in ours. Do we have an ability to send a message and shut down their systems or look like a big accident that turned you know that, you know that looks a little bit like what we just experienced last night. Is it your experience with UK perspective, in your former role that you can deliver a punch to Vladimir Putin?

Sir Jeremy Ian Fleming
I think the reality is that we have to increase the deterrence isn't working in this space. There have been moments in the last 10 years, and I think deterrence has worked. I think there was a high watermark when President Obama called out directly to President Xi, what was, what was happening, and eight years ago and now, but that deterrence was pretty short lived. There was some deterrence at the start of the Ukraine crisis. I think, I think Russia, by its actions, we could see that it wasn't trying to spill out cyber attacks beyond the immediate theater. I think some of that has disappeared so, so we don't, we aren't in a situation of moment where we have, I think, reliable deterrence, and part of that is because the thinking and the sophistication around thinking on how we push back just isn't, isn't nearly developed enough now, without speaking too much out of school, too often, the conversation in how to respond becomes a cyber action equals a cyber reaction type conversation, and that's important, but it's not the only way. It needs to be part of a whole of system response. And there definitely is an issue around our risk appetite in Western countries to push back, but we can't do that at the cost of our values, and we can't do that at the cost of legal northern I agree. We have to do that differently.

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

Steve Clemons
So Kent Walker, John Huntsman, I want to get you into this. And I want to say here, we've got this digital stew now. We've got a lot of connected people. We've accidents, we've been having enough resiliency. We've got some bad actors there. And you throw into the stew, you know, kind of put some pepper and salt and a little bit of AI, a whole new coming technological revolution and and we're talking a little about that trust. So how do you take this stew that we have? And you know, Kent and John, you and I both talked about AI and what it can what can be done, whether AI will save us all or make this all worse. Kent?

Kent Walker
So foundationally, the challenge is huge, and as Jeremy outlines, it goes from the the everyday to the nation state attacks. We have experience on our side, and Google has probably most attack websites in the world, but we also keep more people safe than anybody in the world. We have experience, starting back in 2010 with Project Aurora attack coming out of mainland China, that led us to totally reinvent our security architecture with defense in depth architecture, multi factor authentication. These need to be norms for everybody going forward. That's the foundation, because otherwise we're building on a week decades old proprietary infrastructure. They're shot full of vulnerabilities. And then Steven comes to your question, how can I help us turn that around? Reverse the defender's dilemma, where the center has to be right every time, and the attacker has to be right only once. We are optimistic that AI is actually allowing us to make significant, transformative, yet, but significant progress in being able to identify vulnerabilities, patch holes, improve the quality of coding and really be integrated into our network architectures, far more than ever before. Just yesterday, we announced the Coalition for secure AI building on the safe AI framework, bringing together the leading AI developers and increasingly, AI deployers, because it needs both to make sure that we are exchanging best practices. We are finding AI into our everyday security practices, and fundamentally, we are developing secure software supply chains. People think of supply chains the hardware artifact. It really increasingly now is a software question. You are only as strong as your weakest vendor. How do we make sure that vendors up and down the supply chain have a robust set of standards that they're adhering to that's gonna be critical for all of us.

Steve Clemons
How do you rate the government as a partner in that effort? Is the government's efforts. It's a standards at looking at security. I know Ann is great, but Anne's not the whole government. But I mean, are you know, when you're out there and you're trying to create this consortium, is that consortium smart? Smarter than the US government on these issues, smarter than the EU government on these issues? Where are they or are you trying to carve out areas that you don't want those governments to regulate?

Kent Walker
I would say it's gotten a lot better. But I think again, Anne would agree there's work to be done coordination among the federal government agencies, federal and state and breakfast announcement sponsored this morning, working together. Because increasingly, it used to be in

the 60s, two thirds of R and D was done by the federal government in the United States. Now, 80% of R and D is done by the private sector. That's a remarkable shift, and we have to make sure that our mindsets are adjusting to that. So we're bringing the best of us r&d To solve this problem in coordination and with the convening of the federal government.

Steve Clemons
John, you're now vice chairman and MasterCard, but you've served the public, made public services Ambassador Singapore, Russia, China, been governor of Utah. So you've been on both sides now the private sector, and actually been a chief executive of the state, kind of dealing with these issues. And you've lived in Moscow and Beijing, which has an issue. And I'm really interested in this geostrategic moment, which we've known each other for a long time, seems more fragile and uncertain than any time in my career. About when you look forward and what when you look at the world, we're kind of looking at, how do you build trust when there's so many enemies to trust building out there? How do you navigate it? Either you can wear talks and with your MasterCard hat on, or talk, as a governor that was responsible for state was an ambassador in two of the most problematic geostrategic heavyweights in the world, how do we what's our North Star in that

Jon M. Huntsman Jr.
Thank you, Steve. It's a pleasure being with you. It's great being in Colorado. I was chief executive of the state next door, and I'm proud to say I never declared war on Colorado once. I threatened Nevada several times, but the diplomacy always prevailed.

Steve Clemons
But was there hybrid war?

Jon M. Huntsman Jr.
Malware included, why we do we feel so fragile at this moment, and having lived in both Moscow and Beijing, let's just say my phone was a great interest to the FBI when I left Both those jobs is because we feel that we are on defense constantly. You have a phone, you have a credit card, at MasterCard. We obsess about safety. Those two rings in our corporate logo, when they come together, that signifies trust. With trust, you have everything. Without trust, you have nothing. So we feel vulnerable because you have maligned actors in the world, nation states that are willing to take us down. So Vladimir Putin was sitting on the stage, or pakkashev or shoyu, they would say, we're going to take down your country, and we won't even have to fire a shot, because we got rails into everyone's devices, into every town, big and small. We can shut off utilities. We can create a massive disinformation around your election cycles, and we can cause widespread confusion and catastrophe. That's what he would say. So he took the belief that he won amplifier a shot. He can weaken this country through digital means. If Xi Jinping were sitting on the stage, he would say, thank you very much for allowing us to cherry pick, to pick your pocket of leading technologies in IP because we didn't have to pay for it. We took it from you, and through that, we're able to advance an economy that today is second only to the United States. So this isn't going to change. Going to change. The adversaries are moving with rapid speed as almost as quickly as we are. So that then begs the question, what

do we do about well, government produces some solutions, but in typical government fashion, people turn over with regularity, and there's not a lot of consistency and continuity. Where our adversaries have people in place for decades at a time, and they figure out the strategy toward country, A B or C, and they execute with Freedom Act. So how is it that the private sector and brilliant people like Kent and his people can get together with Anne on an ongoing basis to say, what is the governance and the structure that we need to get us from defense to offense? This is going to be the key question going forward, and then, not just domestically, because as governor of a state, you feel extremely vulnerable in this digital world because you've got towns big and small. You hear the chatter going on at the federal level, but it doesn't translate to the local level. And so what do local governments do? They can't afford this kind of support and education, and know how? What do states do so that they're properly aligned with the national vision on getting us on offense, but then globally? So we're talking about trust. What are the institutions of trust today that really matter, that still exists, because there aren't a lot of them, five eyes. They share intelligence. They trust one another. NATO. NATO is such a trustworthy organization. Say what you will about it that Finland wants in a country that hasn't had alliances in a very long time, same with Sweden. So how is it that we create a bulwark of support in protecting digital infrastructure that is equal to what we've done in the case of global security, in a war and peace sense. And I think that will be the next big question from a governance and a problem solving standpoint, what are the structures that will actually get us on offense as opposed to defense? The answers are there. We're going to continue to innovate and build things. But in the meantime, this cyber attack problem, as Kent pointed out this morning, is a ten trillion problem in terms of the impact it's having on consumers and users and lost business. So if it isn't a trust problem, which it is, it's a huge economic hole that's been blown in the country.

Steve Clemons
Well, look, I mean, your company is trying to bring, well, we're all trying to bring a billion more people into connectivity, financial connectivity. We talk about the next billion that would come into essentially modern connectivity. And how you get that right? But I go back again, I know, and you're working on a national digital infrastructure strategy, and I sort of see the problem is both twofold, not only bringing a lot of people externally, around the world, but also what I would say is an absence of trust in significant populations the United States, where there's a lot of understanding that, maybe not even understanding that tech and digital connection help make your day go better. But there's fundamentally this fear of big companies, of social media, of other elements out there. And so as you're thinking the future, you're representing the Bucharest administration and trying to get this infrastructure strategy right, from what are the central features, from your perspective of getting both the American public and the future global public in a place of equilibrium, that's a high trust network, not a high fear network.

Anne Neuberger
So people see that the devices they bring into their homes, from baby monitors to home security systems, into their schools and into their offices, like routers. When people are shopping for those, they have no way to assess, is this device secure? So there's a sense to your point of a lack of trust and a sense of fear, what access Am I enabling to a criminal, to potentially somebody who may be targeting an individual for their political views, etc. So one of the

programs President Biden has launched is essentially an ENERGY STAR for cyber. It's called Cyber trust Mark, where companies that build devices to the US government's cybersecurity standard and get them tested can put a label on them, like ENERGY STAR for cyber. So Americans shopping at Best Buy or shopping at amazon online can look for that label and know this baby monitor, this home security system, this office router, this smart energy monitor, has been tested to meet a cyber security standard as well as transparency on what data is collected. The program was launched last year. It's gone through a number of legal reviews to get input from the public, and is now at the final stage where companies who will be doing the testing are submitting so we hope to launch in October and have products with labels in stores and online by the end of the year, and to ensure that we could bring the power of global markets to that, we did something unusual for the US government, which Kent would comment is unusual, we reached out to the European Union and said it would be better if we were one Transatlantic Market, because if a product is tested in Paris, France, or Paris, George or the United States, it should be able to be sold in both, and that will incentivize more companies to do it. So we signed a joint action plan on a roadmap to ensure we get there, and we're doing the same with other governments around the world. So that's the first piece, reducing the number of devices that can't be trusted because there are billions of internet connected devices that are simply unsecure, and giving people the power and the visibility to look for that. And frankly, companies want that, because if they're building cyber security into their products, they want a way to show that so that the consumer knows and can shop for that. So that's the first part. The second part is the building the rules of the road internationally and enforcing them when we can. You know, Jeremy talked about the challenges of deterrence, and I agree very much that deterrence is broken down in cyberspace for a number of reasons. There's more actors than ever before. You have countries, you have political activists, you have criminals. Today, for example, the United States will be sanctioning two Russia based individuals with ties to the Russian government, political activists who conducted cyber attacks against infrastructure in the United States. And the reason we're releasing their names publicly. And the reason we're sanctioning them is to build some deterrence against those individuals happening today. That's happening today. The next one share their names. Now I would very much there are their long Russian names. So I'll point you to the to the release of it later from the Treasury Department. The third one of that I know that by their monitors. The second part of that is really how you build upon that, on accountability for countries like Russia that harbor criminals and hacktivists. There are already international cyber norms countries signed up at the UN not to harbor actors, not to attack critical infrastructure. And the first steps we've taken to that so President Biden has made a point of when there are attacks by Russia, we have gone publicly with the European Union, in one case, with NATO in a second to attribute that to say these attacks were conducted by Russia, or these attacks were conducted by Iran, in the case of Albania. Why? Because that's the first step to then more complicated question, which are consequences? And consequences in cyberspace are difficult. If an individual based in Russia conducts cyber attacks against the hospital, what is the appropriate response to consequences for the individuals themselves, because we want to deter them, as well as potentially for the countries that harbor them. And finally, I would note that one thing that's really fueled the rise of both criminal ransomware attacks has really been cryptocurrency. It's far easier to hold systems at ransom, and in the US $1.3 billion were paid by us entities in ransom in 2023 alone, that number is fueling attacks,

because every payment incentivizes the next one. So work we're doing just a final thought on that. We work with countries around the world in a partnership the White House forum called the International counter ransomware initiative began with 30 countries two years ago. It's now 72 they'll be convening in person in DC for three days to coordinate on policy initiatives, how we do things like usually partner with the insurance industry to encourage thefts, and what we do to tackle money laundering by cryptocurrency around the world.

Steve Clemons
I hope you'll invite us all to party.

Anne Neuberger
Actually there is a private sector component.

Steve Clemons
Kent, let me, let me come back to the AI question, because, you know, there's a guy named Arno Penzias, you may recall, to set the internet would make dumb people dumber and smart people smarter. I'm interested in the AI world that's coming, and whether or not, are we over hyping the AI problems. Are we under hyping AI? Where does AI take us? You know, from this journey forward, from your perspective, and are we doing it better than China?

Kent Walker
I think we are doing it better than China, but by months, not years. And in some places, the Chinese actually may have advantage over some of the work we're doing in sensor technology and the like. It's hard to say AI is overhyped, but or underhyped, but, man, think about this not just as a chatbot. Think of it as a scientific breakthrough, and not just a breakthrough, a breakthrough in the way we make breakthroughs. This is going to have remarkable implications for science at digital speed. For material science, we are already seeing millions of new materials. Imagine batteries that weigh attempt as much and hold 10 times more energy. Imagine changes in quantum computing. We're already seeing breakthroughs in healthcare, where we were seeing generational leaps in how we are able to understand how proteins work in the human body, the potential for accelerating energy production, grid efficiency, going through the list of the UN Sustainable Development Goals, AI is a major contributor, will be a major contributor to almost every one of those. So if I had to sum up the opportunity, the stakes of getting this right, I would go back and sounds a lot. Go back 400 years to Macbeth. There's a scene in the, I think, act one, where Banquo goes to the witches and says, if you can look into the seeds of time and tell me which will grow and which will not speak, then to me, Well, that's what AI does, because it's seen a billion seeds. It knows. It can predict which will grow and which will not it is, in short, a tool for predicting the future. Think about that. What would humanity give to have better tools for being able to predict the future? How drugs will interact with the human body, what new innovations we might have to transform the way we do nuclear fusion? It's an extraordinarily exciting time, and so even as we focus on the risks and the fear and the need for responsible and balanced innovation and regulatory frameworks, we can't we mustn't lose sight of that North Star, the potential for incredible abundance that will be so transformative, not just for people United States, but for people around the world. We've already,

in the last 20 or 30 years, because of the Internet and other technological innovations and trade and other sorts of international accords brought more than a billion people out of extreme poverty. That's unprecedented human history, and that's just the start.

Steve Clemons
Jeremy is the AI cat already out of the bag that can't be put back in. Michele Flournoy, what a great piece in Foreign Affairs magazine, kind of looking at the Ukrainian Battlefield, the digitization of war, if you are. And basically said, Look, AI is already at work for us, or work for the Ukrainians in the battlefield in important ways. And I'm wondering whether our conversation and debate about the impact of AI, particularly national security, but more broadly, is one that's already a bunch of cliches and and, you know, conventional wisdom that's so outdated given what's already unfolding in AI. You know, given your worldly intelligence, I look at your intelligence, I love to get your sense of it.

Sir Jeremy Ian Fleming
I'm wishing that I had remembered more Shakespeare. I mean, so clearly the cat is out of the bag AI as a term is, is something that we're all massively overusing, and in some ways that is contributing to the lack of trust in technology is very hard for individuals, for technologists, for policymakers, individual companies, to get up and talk about it in a way in which people society can engage with us. So I I believe that we have to have a different type of conversation as a society. The way in which I talk about that in the past is that is to talk about a license to operate. So what is the license to operate that we really want to have for this next generation of technologies, and how can we go about creating that? And the reason I use that language is because I think it makes it much more practical. If we can talk to transparency, we can talk to legislation, we talk to regulation, we can talk to the conversation that we know we need to have with society we're not having. So on terminology, I agree with you on that, in terms of where the technology is taking us in relation to national security. Well, aspects of AI machine learning analysis have been in and around national security for decades. I very soon after I arrived in GCHQ, I pulled together my people working on AI, and I said, right, tell us what we're doing, how we're accelerating. And I paraphrase, but broadly, they said, don't worry. These are the same algorithms we've been working on since Alan Turing's here. And of course, they that was a bit a bit too attracted. They didn't really mean it, but national security in relation to AI is, of course, a massive thing for us all. It provides great opportunities for us. I think at the moment, the advantage is still on defense rather than offense, but with the next generation of tools coming through, when you get agency, when you're in the space that Ken's talking about, we have to start worrying about that more. And if there's a single thing I worry about is that the pace of our institutions in being able to keep up with this, it's very challenging for how you work.

Steve Clemons
We're nearing the end of the program. But John, I want to ask you the question. I'm going to try to frame it. I think, you know, there was this cover story in Wired magazine in January of 2001 written by Bill Joy. And the cover said, The future doesn't need us. And it was looking at the advances in microcomputing and nanotechnology and biotechnology, and said, We're advancing at such a space now. This is, you know, 20 some odd, 24 years ago and and the point was that

people, individually will become less and less significant in the equation of the advance of technology. You want to major, you help on a major, major company that's out there that's consumer facing, and you're consumer facing when you're a politician, kind of dealing with, you know, constituents and voters. And I think the anxiety of a lot of individuals out there is that they will become the victim of the algorithm. We talk about algorithms doing good things, but people fear being demeaned, neglected, or victimized by some computer system they don't understand. And so I'm interested in a world that continues to bake people into it, versus having the world done to them. And how you navigate that?

Jon M. Huntsman Jr.
Well, first of all, I don't know of a system that is capable of compassion and love and yearning of hope. Those are all human elements. And to use a line out of Shakespeare, sweet, are the uses of adversity. So we'll be knocked down as technology advances, and will come up shorter and smarter and faster as a result. So it's all in our ability, through great innovators and great research universities, funding of the right kinds of talent and technology to stay ahead of the race, but always ensuring that there's a human element with compassion, wisdom and insight that I'm not sure we're ever going to be able to replicate. But there's one thing that I think we need to bring into this equation, because while AI and technology will allow us probably a little bit longer, you can imagine breakthroughs in human disease occurring that will be terribly meaningful for all of us in this room, and well beyond cures for cancer and things like that. But what good does it do to have a longer life if we can't love one another and we can't reason with one another, and I'm thinking about the next billion or 2 billion people that come online. So if we look at the global south, from the archipelago of Indonesia, through the Malacca Straits, through the Bay of Bengal, through the Indian Ocean, the Arabic sea, and into Africa. That's our tomorrow. You have most of the populations there that are not connected. I was in Mexico City a few days ago dealing with the welfare bank in Mexico. We got 20 million cards in circulation to try to help stimulate economic activity. Guess what? They don't trust their banks, and they don't trust payments. So what can we do in order to make sure that we build trust and resilience into the work that we do to bring the next billion to 2 billion people into the world in a way that speaks to confidence, growth and safety? Because if you can't accomplish that, you've got a much more difficult world to manage than the one we have today.

Steve Clemons
We have two minutes left. I'm just going real quick. Ken, I'd love to get your thing. If there was one thing that we didn't get to in this conversation, particularly about keeping people in the aspirations of people like people like people in this room, you know, part of the not only part of the equation, but driving the technology equation more. What did we miss?

Kent Walker
Look, I think the events of the outage last night, the issues we experienced this morning, reaffirm how much digital has become part of daily lives. You think in your hotel room, millions of people around the world can't get on their planes. We depend on these tools. We have to treat them with the level of seriousness that that suggests AI gives us another way, a new maybe

generational change in how we can make security for those tools match their abundance potential.

Steve Clemons
Anne let me ask you the same question.

Anne Neuberger
As John said, digital systems have brought so much beauty to human life. When you think about a child living in a remote part of the world where they may not be the best teachers, access to education, people in parts of Africa, access to medicine, but with that importance comes security people can trust systems. There's an us, and then aspect to that us, the work we need to do to build the security and resilience into systems, and playing to our strengths of innovation and using tech for that, is something where a partnership between government and private sector, government, R and D investments, company investments, AI, can certainly help us. And then there's a them, as Jeremy talked about, building deterrence in cyberspace. There's complexity to that. There's no borders to that. But doing the hard thinking to say, what does that look like for the actors, for the infrastructure and for the countries, will be key to building trust. Jeremy, last word.

Sir Jeremy Ian Fleming
A trusted technology, digital ecosystem, is a fundamental part of our offer to those parts of the world that are looking at us at the moment and saying, What's in it for that. So I strongly believe that how we develop trust in this underpinning, foundational level of our lives is going to define the extent to which we're able to project our power, maintain our security and be prosperous, but with a much broader set of countries as they buy into that trust.

Steve Clemons
Well, I'll just say finally, you know, I often try to think about the public policy world and challenges. .If gravity was just naturally taking us to a good place, we wouldn't have to have a conference like this or discussions like this. It's going to require deliberate work and debate and exchange. I want to thank sir Jeremy Fleming, Anne Neuberger, Kent Walker and Jon Huntsman, Richard for sharing their thoughts with us today.