Cyber Intelligence: An Enabler of Security and Resilience
Wednesday, July 16, 2025 - 4:10 PM ET/2:10 PM MT
https://www.youtube.com/watch?v=gHNA9Ha0oM4&list=PL7fuyfNu8jfP8TWSJzPCsyScNGwbW6xbQ&index=16

Speakers

- Johan Gerber, Executive Vice President, Head of Security Solutions, Mastercard
- Rob Joyce, Founder, Joyce Cyber; Former Special Assistant to the President and Cybersecurity Coordinator, U.S. National Security Council
- Jenna Ben-Yehuda, Executive Vice President, Atlantic Council
- Moderator: David Sanger, The New York Times

David Sanger
Well, thank you. It's great to be back here at Aspen. Great to be with this panel. I thought there for a moment that Chris Bruce was actually going to explain what happened in New Jersey. I And but, but no, we're gonna get him at the cocktail parties and figure that out. We do have a great panel here today. And you know, there was a moment I've been going to Aspen security forum since they started, and you may recall that for a number of years, it was very focused on counterterrorism, then it became very focused on cyber. Then the world changed a bit with President Trump's first term, and we've begun to deal with a range of issues, but we've never left the cyber issues behind. And I would say what marks this year is that we've had a lot of surprises along the way. Obviously, AI is changing the nature of of the cyber warfare elements, and we'll get to that in some time. Obviously, China's salt typhoon has made us recognize that the era of state competition is not only here, but persistent. We've seen rises in ransomware and President Biden's efforts in his one meeting with Vladimir Putin, which was four years ago, last week or so, or two weeks ago, to cut off the Russian based ransomware has not worked. So we're at an interesting cross point here, and I'm hoping that we'll be able to go play some of that out. I'm going to start on this with Jenna, who I'm going to ask, Jenna, you're at the Atlantic Council, you guys have done a fabulous job, I think, of placing cyber in the broader geopolitical competitions. We thought in the early days of the Ukraine war that we were going to see cyber, more cyber activity by Russia against us. We did see a lot of it, obviously against the Ukrainians and the Ukrainians on them. But give us just a little picture of where you think this fits in now to the big global competitions that we're seeing underway.

Jenna Ben-Yehuda
Thanks, David. It's great to be here with all of you and with these great co panelists. So the world is a messy place right now, right we have no shortage of geopolitical instability in contest. We have a land war in Europe. We have war in the Middle East. We're coming off the heels of Israeli and US strikes in Iran, and we have this ongoing aggressive contest for the commanding heights of technological change, and amidst all of that, as if it weren't complicated enough, we have this really broad, based and deep deficit in trust, people's trust in their governments, governments, trust in each other, and trust is a really critical element to cyber and so As we think about the kind of core underlying components of what is required to really manage this

relatively new domain. Consider that NATO only recognized cyber as a domain in 2016 and especially the nature of the private sector engagement in this domain. So it's not one that governments control exclusively, or even always have a dominant sense of authority, and you get a pretty sticky situation. That means that there is a lot at stake when it comes to cyber, and at a moment where a lot of coordination and governance and clarity about standards and authorities is needed, we have governments themselves retrenching from that and private companies demonstrating some understandable nervousness about what their own roles and responsibilities might be.

David Sanger
And do you have a sense generally as the companies have this nervousness it is that they are going to be pushed too hard into offensive cyber responses, or do they think that the government's own hesitation to go finance CISA, the chaos that we've seen take place at the NSA, where, of course, the director of the NSA, and also is the commander Cyber Command, was removed months ago, but has not been replaced. Are they fearful that the government is no longer there for them in a way that they had been in the first Trump administration or during the Biden administration?

Jenna Ben-Yehuda
Well, consider that the CISA act of 2015 is up for renewal. This is a framework that essentially provides insulation and protection for private companies as they can share intelligence with the government without fear of reprisal. That is up for renewal, and it's not a fait accompli that this is going to get done. So this is basic blocking and tackling of governance within the US, just a foundational element of a substrate of trust that's required. So there are some very basic elements for the private sector that have got to get locked in in order to build confidence and ensure that the burden, the cost, the vulnerability that might come with sharing is a measured and balanced one that can be explained to investors and shareholders alike. So right now, even something that fundamental to this ecosystem is not certain.

David Sanger
Let me pick that up with Rob Joyce, who the founder of Joyce cyber, but he was Special Assistant to the President of the National Security Council during the first Trump administration. But many, many years at the NSA in a range of roles, from offensive to defensive and Rob, I think it's the first time we've been on stage since you've left the NSA, but I have to thank you, because I know there were moments when I and my colleagues tested your patience a little bit with things that we publish, and yet you are still willing to talk to us, so I do appreciate that, and we've learned a lot from you along the years. So you've had a lot to say in recent times about our discovery that cyber is not a terribly effective tool of deterrence. And it's interesting, because I think at some of the panels that we were on here five years ago, there was an assumption that you could make cyber a tool of deterrence. What did we get wrong?

Rob Joyce
So great question, David, and there's strong opinions across the board on this, but, but I think it is cyber is a component of deterrence, but cyber, in and of itself, isn't deterrence alone. So if you

think about it, there are various levels we can achieve. We can achieve friction in cyber operations, so we can make it harder for governments or even criminals to come at our capabilities, and we want to challenge them so they don't get to try over and over and over again until they succeed. So that's kind of the base layer is friction, and that a lot of that is in the cyber com doctrine of persistent engagement. We're going to challenge them. Next layer up is disruption. I'm going to take away their infrastructure. I'm going to, you know, take away their tools. I'm going to do everything on a spectrum of, you know, getting them ejected from their botnets all the way to I'm going to discover and turn over their tools so that the commercial world can find them in other places. And then the next layer up is that offensive cyber destructive level, and whether you go against the governments that are doing it, or even all the way into critical infrastructure, saying, I'm going to deter them because they're afraid I'm going to cyber them mightily. Right at that point. Are you going to scare them enough with your cyber capabilities that they'll stop? And I would offer you know, we've just come through a couple years where the Chinese had tremendous success in old typhoon, pre positioning into our critical infrastructure and salt typhoon getting into telcos, and the response from us being on the receiving End of those successful operations was not to go over into the corner and rock back and forth and cower because of the cyber power coming at us. It was to get angry and to start to push back, right? So, you know, I would argue from that test case, cyber is escalatory when you're using it in an offensive way, in those manners, right? I'm not saying we shouldn't do it, but it is a piece of multiple things, and I think there are other levers that push strongly against other nations doing cyber against us that we have to use.

David Sanger
So let me push you just a little bit on the salt typhoon and volt typhoon lessons here, because if there were graduate students in the audience, and I hope we have some this is like the greatest case study in what you were just describing. So first comes vol typhoon, as you said. This is persistent entry, but not necessarily code sitting around inside the utility grid. And it was discovered by the US government several years ago, it became more public, although they were reluctant to discuss it very much in detail, two summers ago. And yet, when you talk to utility executives, they tell you, we think it's still there. And then in the interim, we got salt typhoon deep into the telecom system, able, we don't know if they did it to get into the actual calls that the President Elect or presidential candidate and vice presidential candidate were having inside some of the lawful intercept systems that Justice Department was running. Both of these are Chinese groups, different Chinese groups, but both of them are. There was a sense as the Trump administration came in, that the problem with the Biden administration was they hadn't pushed back hard enough, and they were saying things like, watch just watch this space. You're going to see a lot more offensive cyber. So first, what did we do wrong? If anything on Seoul typhoon and vault typhoon. And tell us a little bit about what you think they mean when they say we're going to go on the offense.

Rob Joyce
Yeah. So, so let me start at the first part, which is, I agree with the premise that we haven't done enough. You know, we have, in the case of the infrastructure, pre positioning, you know, digital explosives being strapped to not only electric grids, but pipelines and transportation and other

critical infrastructure, water, right? Those, those are digital explosives being set and pre positioned. Right? If that were done in the physical world, right, we wouldn't have talked for a week, let alone a month or a year, right? And we would have used a lot of coercive tools. You know, many of the kind of things we talk about here at Aspen, right? There are diplomatic measures, there are sanctions, there are tariffs, there. There are law enforcement tools, their diplomatic tools. We have a wide array of things we do when another country is behaving beyond the pale, outside of the norms, or doing things aggressively that we would not condone, right? Even the simplest terms in the espionage world. So salt typhoon, you know, one of the most basic tools we have when there's espionage plot is we eject a bunch of diplomats from embassies, right? We've not done diplomatic expulsions, right? That's another tool. We have this wide array of tools. And my point is, if we are offended by these cyber operations, we need to show it with all of our government might, and that usually involves, you know, we need to turn things up to 11 and use the whole quiver of tools in in our arsenal.

David Sanger
So one more for you, and then we'll go on to Johan on what's happening in the private sector. I went back. I couldn't find a single time that President Biden talked about soul typhoon or volt typhoon in public. It was a big deal. And you remember, you and I may have discussed this around one of the the Aspen cyber groups, when there was public congressional testimony in which the FBI director did it. But if you stopped 100 people on the street in Washington, and, you know, probably in downtown Aspen, and you asked them what cold typhoon was, they probably think was a new Superman movie. So, so have we sort of failed to learn the lesson of even just getting out to have top leadership talk about it?

Rob Joyce
Yeah, and that is certainly one of those items, I would say, if we're serious and going to dial this up to communicate our displeasure. We do it through multiple channels.

David Sanger
Johan, so you're watching this from the world of MasterCard, where state on state cyber is a problem that you're interested in, but you are the target every day of all kinds of different ransomware groups. Obviously as I said at the intro, the ransomware problem has not gotten any easier, even though there were some very creative things done by the FBI and other groups and system, we have seen the North Koreans continue to do pretty sophisticated cyber crime using cryptocurrencies, and then you've just seen the ordinary, everyday kind of fraud issues that you've long had to deal with that are enhanced by cyber and increasingly enhanced by AI. So tell us just what the threat matrix looks like to you right now.

Johan Gerber
I can probably sit here for the next two hours talking through all those topics, David, but thank you for the opportunity. You're right. I think the world has become increasingly complex and interconnected. You know, the world is now more connected than ever before, and every minute that we sit here that will just keep increasing, which means the the fluidness of how these attacks goes back and forth between what happens if you have a geopolitical motive or a

criminal motive. These lines are all blurry, which is why, as a company, we feel it's so important to be in the middle of cyber. Many folks think of us as a payments company, but if you think about what we're doing, we're connecting 3 billion consumers with about 150 million businesses across more than 25,000 financial institutions around the world. Everything digitized, it is, it is a frontier where every possible way of cyber attacks. We see them, and we feel that there is a real need to collaborate as a private industry, a public industry, together to fight these things, to defend, but also very much to deter this. You know, we work very closely with law enforcement. We want to make sure that we that there's a consequence for these criminals if they do these things. That's important for us. As we look at the other world is evolving now we see all sorts of new payment types. You know, I'm proud to say, if you think about the card industry, it's built on the on the on the principle of trust, and that's manifested every day when you use your card, either to go into a store and you tap that card on the device, or you click Buy in an online environment, what happens is there's a fundamental promise that the business was selling you the goods will get the money and use the consumer are protected. That's why trust is such an important piece. And Jen and I had this conversation for a long time this morning. That's why us in being involved in things like Aspen, being involved on stage here, is so critical. Why we want to reach out to governments all across the world to say we have to do this collectively. We have to push back against ransomware, ransomware on small businesses, for instance. Just to go down a little bit of a rabbit hole here, we've done a study. Small business is still the largest employer around the globe. You know, MasterCard was a small business at some point in time, Google was a small business, Microsoft, Amazon, they were all small business at some point in time, more than 60 46% of all Smith small businesses are attacked every single day on a cyber front. 60% of those who are getting attacked will go out of business because they don't have the resources, the funds to withstand or sustain them. How do we come around to wrap our arms around those? Because that is prosperity for the world. That's our next generation of employers that's out there. For that reason is why we are so deeply involved in this. On the card for side, what we've seen, and what worked very well is when you create an ecosystem where there is liability and a reason for investment. So for instance, in the card industry, as a consumer, when you use your card and there's actually fraud on it, the liability for that fraud goes to the least secure party. So if the business is selling you, businesses did not implement the latest technology, they will suffer the loss. If it's the bank that didn't the bank will get the loss. We need more of those regulatory frameworks in our systems to generate that motivation for people to invest in embedded security. Embedded security for us is fundamental if we want to get the benefit of what the new technology innovation brings. Ai, you know, quantum, holds great promise for mankind, but you will only get the benefits if security is embedded. Otherwise we will. We will lose the trust. I'll give you one more example. We had a pledge a couple of years ago. Mascot pledged to bring a billion consumers into the digital economy. The biggest question that we had was, what is their first experience is that of a scam, an online bullying or some sort of a ransomware attack, we will lose those consumers in those communities forever. So the embeddedness of this and this is something where we think industry has to do more. We feel that the relationship between private industry and public industry needs to strengthen. We need more harmonization. Fragmentation is a big deal for us, and I hope we will get to that conversation a little bit later today. But the world is connected. We can't move away. So even if we see more sovereignty, or drive sovereignty, the world is never going to be less connected

than it is today. So we really need to keep driving a better harmonization across this across this line.

David Sanger
Johan, let me ask you one specific and you just alluded to it before, which is the effects we're seeing from Ai. So I think from one of these stages, I think two years ago or three years ago, we had some of our friends from Microsoft up here who are basically making the argument that they thought AI would help the defenders more than the offense. But as we were all discussing before we went on stage, I've had the sense that may be shifting now. So what are you seeing? And then I'm going to ask Rob to go in on that same question.

Johan Gerber
Yeah, I need you to give me a shot before Rob goes on, because he's going to really scare the hell out of everybody. But I think you're right. I think there's a nuance answer here. It depends on how much we're willing to invest in AI. You know, we've seen great results from using AI as a defensive mechanism. We use that every single day, every single day, somebody uses a payment instrument, whether it's us or one of our competitors. You will see AI at work to defend and protect those those transactions all the time, but we are seeing that the the offenders and the ones who are using AI as an offensive tool, they don't adhere by the same rules. There are no borders, there are no regulations, there are no rules by which they play, and that for some reason, they collaborate amongst one another way more than we do. I can tell you when we see an attack, a successful attack happen in some part of the world within minutes. That whole modus operandi is propagated through the entire underworld, and everybody's got access to that technology. They share. They don't believe in IP rights or anything like that, even amongst themselves. So we have a real challenge in our hand, and if we do not invest in cyber or in AI as a stronger defense. I think you're right. We have a real danger that the on the offensive side, the shift will happen very strongly.

David Sanger
Rob you've always made the very subtle and nuanced point that one of the problems of the United States is that we actually suck at patching. I think you've used that phrase many times. Is AI going to solve that problem in any way you think?

Rob Joyce
No, I think it's actually because of AI. The patching challenge is going to be worse. And why do I think that AI is getting exceptionally good at writing software these days? That means to write functioning software, you have to be able to debug it. You have to be able to find flaws. And what we're learning now is you can turn AI onto software to find vulnerabilities, which are the intro step to making exploits that hackers will use to exploit and compromise networks. So what we're seeing is we are in what Sandra Joyce coined this week at discussions here the AI before times, we're starting to see those technical capabilities without the actual operations. But what are the signs? One, there is a vulnerability database that is enumerated by miter to keep track of all the vulnerabilities in our software and chat, GPT four Oh was able to reproduce exploits in 80, 87% of the cases where it was given the description of the vulnerability, but not even the

software, right? So that is an impressive ability to just recreate exploits. In the case of a company called hacker one, where they crowdsource hackers to Red Team companies, with their permission, they keep a leaderboard of who's the top hacker, and it's, you know, it's credentials and monetarily rewarded to be on that on that list, the number one hacker for hacker one is now an AI bot called Expo. So Expo is out there, 24/7 going through the list of companies who have signed up to be hacked. And it is beating the humans there, and it's getting that at scale. And doesn't, doesn't take vacations, it does not and then the last example I give is a company called hack in the box runs, cut, yeah, they run Capture the Flag challenges, where people get together teams of hackers to go try to solve a hacking problem. And they ran a competition in March of this year, which is 15 years ago in AI, in AI years, right? So, March of this year, the competition and AI bot finished in the top 5% of that against 400 human teams, right? So it beat 95% of the human teams, not people, but the teams of people collaborating on hacking challenges. So it is showing that these AI capabilities are very, very capable, and as each new foundational model comes out, they're only going to get better. So your money is on offense at this point, I think, I think offense has a tremendous advantage. I still believe whoever uses AI is advantage, right? If you, if you have a defender using AI against an attacker who is not, they will, they will succeed. But the AI attacker against people who are not using AI to simultaneously find the flaws before the attackers do, they are going to win.

David Sanger
Jenna, you had a plan on this, and then I have another question for you.

Jenna Ben-Yehuda
I just wanted to come back to the comment on small and medium businesses and connect it to AI, because I think it's so important that we we talk a lot about private sector cooperation on cyber. There's a huge range when we talk about private sector Mom and Pop bakery to master cart. So huge differentiation in terms of the level of sophistication and resources to prepare and respond to cyber incursions. And right now, we've got a huge risk of these small and medium sized businesses really being way left behind in the advent of AI. They're already making decisions. Gosh, I'm barely making rent. How do I invest in a program? Even though, as you point out, Johan, these can be existential moments for many of these, especially small companies. So it's not just a good thing to do to fix because it generates tons of jobs and is a driver for the US economy. That alone should be enough, but there are also huge sources of threat intelligence that we're not pulling in in a systemic way, and with the advent of AI, we risk a huge bifurcation in the ability of the private sector to respond. That's pretty scary.

Johan Gerber
It really is. And, you know, on that topic, I think it's an opportunity for government, private and NGOs to all come together. We see a lot of NGOs doing wonderful work in collating tools and creating free resources, but we need to get them to the small business, you know? And we said, Where are the concentration points? Telecommunications. They all need connectivity. They all need finances. They all need something. And those are the concentration points where we need to embed more of these things. To ask a small business owner who runs a bakery shop or or hair salon or whatever it's out there to understand cyber it's almost impossible. So I think we

have a lot to do in the industry, of the of the of the interest of the economy to help drive and just make it more secure at the at the base level.

David Sanger
Jenna, here's what I was going to ask you. We've all been saying since, really the Obama administration, that the key for cyber is to integrate it with the rest of our global strategies. That, as Rob points out, you can't use it as a deterrent alone, but combined with your nuclear force, your drone capability, your cyber you can, you can integrate this all together. And I think that was true at the end of the Obama time. I think it was certainly true in the first Trump administration, when I could walk over to the White House and talk to Rob and his colleagues about this, or I could go to the NSA later on and talk to general Nakasone about it, or you could go to CISA and talk about defense and so forth. And that continued, in fact, during the Biden administration, when Ann Newberger was the Deputy National Security Advisor for cyber and emerging technology, a job that does not exist right now, I have to say, I've covered this for a while. I have a hard time going figuring out who to go to that's going to drop this into into the larger run. Is that a temporary thing, or do you think that we are for the next few years? And I'm sorry there aren't people from the administration here that I can pose this to, so you're going to have to answer, not on their behalf, but just your view of it is that just something we're gonna have to get used to here.

Jenna Ben-Yehuda
Well, cyber is part of all domain warfare. We're in the moment of all domain warfare. You don't, you don't get to pick and choose your domains anymore. And so I think what you hear is a real hunger for rules of the road. And there are some very big questions, I think I would posit they are inherently governmental questions to answer about authorities, about standards. Folks need to know if their participation is going to be welcome or if they're going to get slapped with a fine and they're going to be on the front page of the paper the next morning as a result, for all the wrong reasons. So I think what you are experiencing, and what I certainly in my conversations with folks here just this week, is this palpable sense that there is more structure and guidance and a framework around which this can operate. There is a real hunger and a deficit for that. And it's not just in the United States, we're fresh off the heels of the NATO Summit in the Hague, where we had a 5% agreement. Huge news coming out of the Hague that was not foretold six months ago. And 1.5% of that 5% is about infrastructure. That is a cyber dividend. Very much could be so, I think, but that relies on Anisa, the kind of scissor counterpart in Europe, and NATO, to join forces in a way that would also be unprecedented for cooperation. So this fragmentation, that is a very real element, is not just a US challenge. It's a global challenge. But there is a hunger, I think, on the part of so many stakeholders across the space to see some convergence in that area, to get things done. Because you cannot handle these issues alone.

David Sanger
We only have about two or three minutes left. So I'm going to ask first, Johan, as you look at this from MasterCard run you would interact ordinarily with many in the US government and obviously in Europe and Asia on this do you find that interacting with the government on these issues has changed in the past six months, since CISA has gone through the budget cuts it's

having Since the NSA and others have gone through their issues. I've been recently with some US contractors who are working for the intelligence community on this, and they tell me they feel a sort of absence of direction. Are you seeing that?

Johan Gerber
Yeah look, I think by nature, there is because of the changes in the personnel. You know, just getting to the right people is a little bit harder than it was. But I don't think that there is a, I would not categorize it as the administration has a lower emphasis on cyber. I would be, you know, a lot of the conversations we're having them, cyber is still a, still a very big focus areas for for the administration. There's still ongoing conversations that we have with them. There's still a lot of business conversation we have with multiple governments around the world. You know, a Recorded Future is a company that we acquired a couple of a couple of months ago, about six months ago, they threw those channels actively engaged with government in a lot of actions. So I still think there's that. But of course, there's a different there's a different framework now and how you communicate with the government, and that certainly is

David Sanger
true, and rob our last question for you, if we somehow yanked you out of your happy retirement and put you back? Not happening, not happening. We're doing this as a hypothetical, okay, because now that you're out of government, you can't use that line. I don't answer hypotheticals. Well, I guess you could, and you had to identify two or three big issues in cyber that you think are quite urgent for the administration at the highest levels to go deal with over the next 12 to 18 months, recognizing the overall geopolitical chaos that Jenna described so well. What would those be? Front

of the list is talent, right? We've lost a lot of talent in the downsizing of the government, and the most capable folks in the cyber arena have the options into the private sector, and so we really have lost some talent. And so it's it's making sure that we continue to build that bench and get people in the chairs that can work across government, across private industry, internationally and with academia. Second thing is, I do think we've got to continue to refine that strategy. What are we going to do in the space of cyber deterrence, and that includes offensive cyber and all of the other things. And if you if you look at where we are, defense has gotten so much better in the last decade, but I think offense has outpaced it. If you look at the ransomware numbers and other things, and then look at the Chinese intrusions. You know, we are continuing to slide and the offense is having more wins than defense. So, so we've got to, we've got to double down on that strategy. And then finally, I think it's really staying focused on the AI challenge, we have the leading AI developers, all of the best companies, doing the most innovative research. How do we make sure that defenders and the government get the maximum advantage out of what they're doing in a way that is really, really effective, so that we can keep the offense from being able to leverage it in a way that they have the advantage. Great.

David Sanger

We have just maybe two minutes for a couple of questions, really quick, short questions, if anybody's got something urgent right back here.

Steve Shapiro
Thanks, David, Steve Shapiro from the Atlantic Council, and Ben, just an observation as to offensive defense and what one could do. Just a note, NATO doesn't do offensive cyber. Just sit on that for a while.

David Sanger
That's absolutely right. And in fact, their defense has usually been changing now, but largely just defending their own networks, any others?

Ellen Nakashima
Ellen Nakashima with the Washington Post, thanks for a great panel and discussion on the question of deterrence and and doing more in offensive cyber. You to take volt typhoon for for instance, digital explosives pre position in critical infrastructure, including, you know, in your American military installations, I think some on the Hill would say, Well, why don't we just do it right back to them, you know, go pre position, our digital explosives in cyber in their infrastructure. Rob, could you talk a bit, a little bit about how you all would think about that as in terms of potential options for deterring an actor like that would pre positioning digital explosives in another country's critical infrastructure even be something you might Consider, or is that normatively off the table because it's, you know, critical infrastructure that affects civilians.

Rob Joyce
Yeah. So I certainly can't speak for the administration. They've made some statements that sound like they, you know, they intend to pursue and examine that, but you know, we haven't seen the results of those deliberations yet, but I still go back to the point of, you know, we have it on our infrastructure, and that has not deterred us. So I don't know why you assume that if we do it to others are going to be deterred. I think we have to use offensive cyber to to to disrupt their activities, but then we also have to have all the other tools in the tool box to really convince them that they they should be deterred from these actions,

David Sanger
and you need a way to escalation dominance if they do come back. Well I want to, I got a million more questions for these three, but we are out of time, but I want to thank you all for great conversation.