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

Thursday, July 20
4:00 - 4:30 PM MST
Democracy, Security, and Artificial Intelligence
Rob Joyce, Director of Cybersecurity, National Security Agency
Brad Smith, Vice Chair and President, Microsoft
Moderator*: Susan Glasser, Staff Writer, *The New Yorker

Susan Glasser:
Hello. Okay, good. You can hear me well. Thank you, Neve. Uh, thank you to that last panel. I have to say, this is another one of those challenging assignments, right? We've been given the task of discussing democracy, security, and artificial intelligence, and we have half an hour including your questions. So I'm sure you guys can be very brief and concise and, uh, you know, let us all have it. But no, actually, I'm, I'm delighted to be doing this one because it's one of those panels where I wanna know what you have to say. And I have a feeling we're all gonna learn a lot from this conversation. Uh, everyone here is gonna wanna hear your observations, both of you, because you've been at the front lines on the sort of generative AI conversation. But I think we should probably start out, uh, you know, more in the realm of the present day and, uh, you know, the, the world of cyber threats as we've seen them right now.
And then we can talk a little bit about the future. Uh, Brad, uh, Microsoft has been in the news recently with the latest round of hacks. I think it's hard for many laypeople to make a distinction. Uh, you know, what really matters, what's different this time. Uh, we just heard a little bit about the war in Ukraine, about China. Tell us about this latest, uh, attack from your perspective, uh, from China and what it, and, and especially help us to understand the context in which we are now seeing, uh, a new generation of threats from China. What's, what's different right now?

Brad Smith:
Um, well the first thing I would say, in addition to just, uh, how nice it is to see everybody here and be here with you and, and be here with Rob is yeah, I would start and look at the broad landscape that exists today. And I would say there are four types of cyber threats. There is espionage, base based intrusions designed to extract information. There are malicious attacks designed to destroy infrastructure. Uh, there is ransomware designed to in effect extort money. Uh, and the fourth I would put in this in a similar category is, uh, there are cyber influence operations run by governments such as China, Iran, and Russia, uh, designed to get out messages and we should think of them all together. Now, to answer your question, uh, what

was in the news this past week, uh, was really about the extraction of information, right? The intrusion into networks, um, with, I would say growing sophistication, uh, you know, all designed and in that case to extract information from unclassified email systems

Susan Glasser:
Mm-hmm. <affirmative>. And was there, I mean, obviously this, for this Aspen security form, it's a group that, uh, is very interested. We have Secretary Blinken coming here tomorrow. The extent to which, uh, you know, this connects up with, you know, just a new and much more, uh, sort of fraught political climate between the United States and China. I, I'm just curious whether there was anything, uh, different Americans are used to reading lots of reports about, uh, you know, hacks and intrusions. What, what made this one different?

Brad Smith:
Well, and I, I really look to Rob, why don't you go first and I'll go second and, and, and maybe put the past month or so Sure. Together, cuz rather than just the last week. Cuz I think it probably should be something that's knitted together.

Rob Joyce:
Yeah. So I think the one you're referring to is where state department and commerce emails along with some others, um, were taken out of cloud infrastructure, right? And so that is one unique thing was the trade craft that, that was able to impersonate authorization to go in and read those emails. So that's one thing, but, but that is a fairly traditional threat, right? Right. It is China doing espionage. That's what nation states do. We have to defend against it. We need to push back against it. But that is something that happens. Um, Brad was, uh, um, alluding to other China actions. We did a joint industry government advisory recently, um, about other Chinese action, which is really disturbing, which is prepositioning in critical infrastructure inside the US critical infrastructure space inside some military unclassified systems. A as well as going after, um, you know, the, the territories that are important in the event of a Taiwan, um, China escalation mm-hmm.

Susan Glasser:
<affirmative>. And tell us a little bit, Rob, uh, about what we've learned from the war between Russia and Ukraine. Certainly it was a somewhat, the expectation before the conflict erupted in, uh, you know, 2022, that we could see massive new kinds of attacks by Russia, not only inside Ukraine, but potentially on, uh, Western allies who are aiding, uh, Ukraine on the United States itself. Uh, to a large extent that has appeared to be, uh, if not something that didn't happen, at least more manageable perhaps than some feared and not a worse case scenario. Can you help

us understand why that is and what we've learned so far from, from the war with Russia and Ukraine?

Rob Joyce:
Yeah, so I'll, I'll dispel the, the impression that there wasn't a lot of cyber. Um, it was generally though confined to, um, Ukraine in the near abroad. And, and it was significant. There were wiper viruses, there was information operation campaigns. Um, there were effects that that flowed into the kinetic space. But, you know, a lot of, a, a lot of praise should be given one to the Ukrainians who are exceptionally resilient when they get hit with something. They've gotten good and practiced and experienced at restoring those systems. And, and we need to take a lesson from that. We need to not only assume that we can stop things, but we need to be resilient after they happen. And the second is the role that industry was able to play, um, in that. And I'll let Brad talk to some of that.

Brad Smith:
Yeah, and I do think it has been an extraordinary collaboration for companies like Microsoft and others together with the US government, the UK government, and, uh, especially the Ukrainian government. And I would say a few things emerge. Number one, we always talk about cybersecurity attacks as if they're based on penetrations into a network while the building in which the computers reside stays intact. Well, it turns out that one of the first Russian cruise missiles took out Ukraine's data center and simply obliterated it. But we had worked with others to evacuate the data. And so I think the first lesson is any country should have a contingency plan so that if there is an actual shooting war, it has that kind of ca capability in place, and the closer one lives to a neighborhood where that kind of war could break out the more important that kind of contingency plan becomes.
The second thing I would point to is I think that we have really seen two very important advances in the last, say, six years. When Rob and I were talking with each other about, say, the not Petya attack on Ukraine, which was really quite devastating to Ukrainian computer infrastructure. The first is the state of the art of threat intelligence, you know, has advanced considerably. So we're able to detect attacks. The whole industry is able to detect attacks to a far greater degree and much more rapidly than before. And the other is what we call endpoint protection. The fact that PCs, laptops, phones, devices are connected, they're enrolled. And what that means is that when they use an endpoint protection service, as we offer, for example, and so do others, when we see an attack, we're able to write code, creates a signature, dispatches it to a device, and then when the malware comes, it's intercepted before it can do damage. So, you know, we've seen some fundamental steps forward that I think have increased defensive capability. And fundamentally that's the story of the cyber war defense so far has triumphed over offensive attacks.

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

Susan Glasser:
Well, that's a great segue to, uh, to this AI conversation because, uh, you know, the good guys and the bad guys are about to get an enormous new capacity where they already have it. And so, you know, I'm sure everyone here wants to, your insights from both of you to help us understand, you know, what does it mean to layer on this kind of a cyber war and then, and then add in, uh, the new capacities in, in generative ri Rob, what, as you look ahead, I'm, I'm curious, help us to understand, you know, what it means for, uh, offense, but also what it means for, for defense.

Rob Joyce:
Yeah, so artificial intelligence, and especially the new generative AI that has emerged, um, is going to be disruptive, right? There isn't a person in this room, a business on the planet that's not going to be, um, impacted in the way it's going to be applied. And, and it's going to have both benefits and risks. I think if you look back at the history of the internet, you know, we, we had this, this youthful exuberance that the internet sharing truth across the world would be the end of dictatorial regimes and oppressive actions. And, and it turns out it's been just as powerful for people who wanna oppress their, their citizenry and want to disseminate falsehoods or false narratives, um, as it has been, um, deli delivering truth. And I think what you're going to find is these new technologies are going to be both, um, an opportunity and a risk,

Susan Glasser:
Okay? But dystopia on steroids or, uh, opportunity on steroids, like in terms of capacities, what, what's interesting is it seems that it will absolutely turbocharge the abilities, uh, of people who wish to do harm that they, uh, no longer will you have a, a, a foreign language hacker who, you know, who's phishing emails are easily detected, uh, because, uh, you know, he or she doesn't, uh, isn't able to write in our vernacular, that kind of thing. Uh, and I'm sure much thought has gone into what kinds of capacities.

Rob Joyce:
So my belief is, at least in the near term, huge advantage to the defense, right? Um, artificial intelligence is actually pretty good at finding material created by artificial intelligence. So we will be able to, um, monitor and look for, um, that malicious content or the things that are happening. Um, I I also think that, you know, the, the resources on defense are much bigger than the resources, um, of the criminals or the small activities, um, that are planning and researching this today. And, and those, those defensive innovations, we're already applying them, we're already seeing them in use, those are going to, um, detect intrusions both classic

and AI driven intrusions at scale. And so I think certainly in the near term, um, the, the, the, the weight is going to be to defense,

Susan Glasser:
You know, um, Brad, you've written in and tried to be very thoughtful in terms of outlining principles that that might shape how we think about, you know, what governments can and cannot do, what individual actors should do in this new AI era. And I was struck by one of your proposed principles, which was, you know, essentially maintain human control, maintain human control. I wanted to ask you how, how feasible you think that is. I guess the scenario that, you know, that I have in mind here is, well, we spend a lot of time in Washington talking about rules of the road or how we should apply principles, uh, and then, uh, we may have other, uh, adversaries who, who don't, who, who don't abide by that.

Brad Smith:
Well, I think let's first start with the principle. I think it's an important one, and it, it has implications that differ depending on the setting. First, there's this question that people ask in the summer of 2020 threes, having seen the rise of things like chat g, PT and GT four. Um, are these machines going to destroy us all? And yeah, I think it's a natural question for a generation alive today, like all of us who've probably been exposed to dozens perhaps of novels and movies that all basically have the same plot structure. Human creates machine, machine just tries to create human, human survives by unplugging the machine. It's amazing how many variations you can do on a plot line that's so simple. But you know, then when you stop and think about it, if that's the concern, and it is a concern we absolutely should take to heart, that's the best way to avoid the problem happening.
What it means is you put in what we call safety brakes. You put it in around the model, you put it in, in the data center infrastructure where it's deployed, certainly for anything that's going to control the electrical system or the water supply or the flow of traffic. And just think that, you know, this has been part of the history of technology since people realized that you could use electricity for something in addition to dodging a bolt of lightning that would electric you, you, you could harness the power and create a circuit breaker to turn it off. You could create a bus, but you wanted to have an emergency brake. You could create an elevator and you would put a safety brake. So put that category in in one, uh, area and say, let's make sure we keep this under human control. Now then when we talk about cyber activity warfare and the like, I do think it is an important principle that we ensure that none of us wake up in the morning and find that machines started a war.
We want humans to remain in control and humans should remain in the loop or on the loop. Now, I'll say the one exception to that is there are areas of defensive activity, defensive activity, where you want ai, I think, to respond to attacks at machine speed. And we've done this even in

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

Ukraine. I mean, we've used AI systems. There was a cyber attack on a shipping company in Ukraine last year where AI saw it and responded before a human even saw it. And so I think defense is different from offense. We should establish norms, and then we need to go to work to do everything we can to persuade every government we can to abide by this norm. And we need to have deterrent mechanisms in place. And this is where cyber command, the Department of Defense, nato, and the like, I think come into play in terms of

Audience question:
Backing that up with deterrence.

Susan Glasser:
All right, Rob, so are you gonna definitively, uh, assuage us from the robot overlord scenario here? Um, you know, it tell us a little bit seriously though, I think Brad's point is an important one in terms of what, what is the level of discussion and, you know, interaction right now around actually creating some of those deterrents? Because it seems like the technology has moved so quickly, it has outpaced at times our ability to, uh, create collective responses to it.

Rob Joyce:
It, it has moved, uh, exceptionally fast, Susan. Um, I think the, the key thing to understand is all of the right people are aligned to work on the problem, right? So in the us the White House leads the task force. Right now, you heard earlier from the office of SI science and technology policy, um, the, the work they're doing to bring together the government in their policies. You heard from our UK friends about their leadership role trying to get the UN to talk about this. And, and we are seeing a, an an enormous amount of government and, um, and, and industry interaction, um, to do a number of things, right? One of the first things we're talking about is we've gotta protect this technology, right? Whether it's from adversarial nations or criminal groups. And so the government has reached out to, um, the, the, the, the innovators of this technology to make sure that the models aren't stolen and then used in, in ways that won't have the kind of, um, controls that, that a company like Microsoft would put on them. Um, we've then started to think about, you know, what are the right, um, policies and norms about their use and employment? And are there places where you need to make sure that a human's in the loop, right? NSA's used, um, AI in our workforce, um, for a number of years, and it never, um, issues a report or makes a decision on its own. What it does is it improves the speed, accuracy, and reach of the humans who make the ultimate decision, but they get to do more because of it.

Susan Glasser:

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

So I wanna ask, uh, if there's anyone in the audience who would like to ask questions, which I suspect will be better than mine, uh, please do introduce yourself, uh, and make it a question so we can get a few. Thank you.

Audience question:
Thank you. Uh, David, I like doing your concerns, citizen. Rob, I have a question you're not gonna want to ask answer, so. Sure. Um, so don't you think that the United States and the NSA should do more offensive operations as a way of deterring China, North Korea and Iran so that they know that we have capabilities. So this sort of thing that just happened doesn't happen on an ongoing basis. I'm glad to hear that defense we're, we're starting to get some more tools, but I, I think the leaders of these states need to be deterred.

Rob Joyce:
Yep. So, so that lane of offensive action is cyber commands and it's the, it's the White House's policy decisions of how, where and when it's applied. But I think if you look, um, cyber commands had an exceptional, um, record of applying offensive capability to everything from the terrorism fight to election interference, right? 2020. Um, they went ahead and worked to take down Perian and, uh, his IRA misinformation, um, capabilities defend the election. There is no doubt China and Russia and Iran understand the might power and capability, um, that the US has in cyberspace and that we do employ it. Um, and it is not the case that cyber deter cyber all the time. So we use cyber as an element of a multiple, um, set of conditions to try to impose good behavior and deter bad behavior.

Susan Glasser:
I'm assuming, uh, Microsoft does not have its own offensive, uh, <laugh> capabil ability to move. That's absolutely, we'll go correct <laugh>. All right, we'll go to the next question then. Uh, you sir, in the back.

Audience question:
Hi again. Uh, Patrick Wilson from Media Tech. So Mr. Director, I'm gonna ask a question that's very keenly, uh, in Brad's area of interest, and that is about workforce, you know, semiconductor companies and, uh, software leaders like Microsoft. We are keenly aware of trying to find the men and women and, uh, engineers and specialists to build this great, exciting future that we've just talked about, but particularly in the intelligence community, I know there's concern, right? That you're competing for the same talent, but with half of all the master's degrees and two thirds of the PhDs and most of these disciplines being foreign born persons, it's much harder for you to recruit. I just thought I'd give you an opportunity to talk a bit about what you guys are

working on, on workforce, particularly on ai, and maybe that would be something that you would have in common.

Rob Joyce:
Sure. Thank you. So the workforce issue is, um, vitally important to NSA and most of the government agencies that do tech, right? Um, the magic of NSA is not in the machines or the capabilities we have. It's in the people because they do the innovation, they do the analysis, they do the operations. Um, we, um, we do really well hiring in two places, excuse me. Um, first is, um, straight outta college, but ex especially people who come in as interns or through things like scholarship for service, which is an outstanding program through the National Science Foundation to identify students and pay for their education. And then they owe an equivalent number of years, um, in government service. Um, those bring us the, the best talent. We also get a number from, um, in, um, from retiring military who have worked in the discipline while in uniform, and now they're ready, um, to have a little bit less movement for their family potentially, or they're just ready to be outta the military and they come over to the civilian side and continue to do, um, things that support the nation.
Um, so we have those efforts underway, but for N S A, we start all the way down to, um, the, the youngest level in the, uh, in the country where we do gen cyber camps around the nation, um, where K through, um, 12 students, depending on the setup of the camps, will get exposed to cyber opportunities, cyber careers. So we push through all of those. You will see, um, the office of the national cyber director coming out with an education and development plan that is key to part of our recruitment and, uh, talent piece. But, um, we put a lot of energy in it, and we actually do really well at NSA of, um, not only, um, recruiting, but retaining, um, because it's no good if you just leak everybody out. I've been with NSA for 34 years, and I, that's not an unusual,

Susan Glasser:
And, and Rob, remind us how big, uh, NSA's overall workforce is now.

Rob Joyce:
Um, I can't give an exact number, but it's, uh, it's, it's tens of thousands of people. Yes.

Brad Smith:
I would just offer a few thoughts to address your question. The first is, especially at a place like the Aspen Security Conference, when there's so much discussion about the US and China, including in ai, everyone focuses on the competition or race as to which country will develop stronger ai. What we miss is that there is a race of equal or perhaps greater importance as to which economy will go faster to use and deploy AI to move the frontier of its competitiveness as

a nation and as an economy. And no one in the United States should ever underestimate the speed at which the Chinese economy, including in the private sector and even the state owned enterprises, deploy new technology. So now bring that to the United States and ask what does it mean for us? One of the things is we need to recognize that AI will change jobs, it will require new skills, and we need to move quickly to, in create in this country the ability of our people to get those skills, to put this technology to work.

Now, I entered the workforce in 1985, about exactly the same time that the personal computer was entering the workforce. My very first day as a full-time employee, I walked into the United States Federal Courthouse in Manhattan as a clerk carrying my own pc. And it was, I think the first time a PC entered the courthouse because I wanted to use it to do my work. Now, what we saw between 1985 and the year 2000 was a rapid expansion of employer spending on employee training so that PCs could enter the workforce and people would train their people on how to use a pc, how to use a word processing program, how to use email, a spreadsheet, all of that. And then we hit about the year 2000 and employer investments in employee training declined for a decade and has stagnated ever since. I think this is a lot like the entry of the PC into the workforce.

We need to move quickly as private sector employers, as governments thinking about workforce training programs. As we think about financial aid for people who otherwise might not have access to this, we need to think about the role of community colleges. We in the tech sector are already creating new curriculum, new programs, but we ought to seize on this as an important part of the national initiative because the jobs will go to the countries where the people have skills to put the technology to work. And we need to be not only the country that creates this technology, but that uses it in every part of our economy.

Susan Glasser:

Well, I think that's a perfect, uh, setup, really. I believe our next, uh, panel is on competitiveness. I'm gonna give our audience a chance for one lightning round, uh, question to, to end this one though. Yes, ma'am. Right there.

Audience question:

Hi, Megan Rested Bellingham. I work for Bridgewater Associates. I do information security. Um, question for you is around data privacy. That's been a big topic of conversation recently. And is there a line that we should draw between technological advancement in AI and keeping people's individual information safe?

Susan Glasser:

So if you can actually answer that in a lightning round, then we'll all be in good shape. I think.

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

Brad Smith:
Yes, there should always be such a line. The line is best drawn by the law. The law is best enacted by Congress. And maybe if 2023 is this inflection point for ai, just maybe the United States can use 2023 to become the 110th country in the world to adopt a national privacy law. Because if we would, then we'd have a clearer line and we would all know where it is.

Susan Glasser:
Rob, a final word?

Brad Smith:
Nope, I agree. <laugh>,

Susan Glasser:
That was truly a lightning round. Thank you.