Roy Azevedo (00:00):

Work. At Raytheon Intelligence & Space, we're focused on designing and delivering the disruptive technologies our customers need to succeed in any domain. Space, air, ground, land, undersea and maybe with most importantly for this next event is cyberspace. We are proud to partner with our nation and our allies to craft solutions to win in that critical cyber domain. And I'm very eager to listen to this next session on just that topic, the intersection of cybersecurity and national security. Neither of our panelist need much of an introduction but please allow me to share a little bit of a background.

Roy Azevedo (00:43):

General Nakasone serves as commander of US Cyber Command, Director of the National Security Agency and Chief of Central Security Service. He previously commanded US Army Cyber Command and the Cyber National Mission Force at US Cyber Command. His most recent overseas posting was as the Director of Intelligence, J2 International Security Force Joint Command in Kabul. He also served twice as staff officer on the Joint Chief of staff. Thank you for your leadership General Nakasone and thank you for being here today to discuss the partnership between Cyber Command and NSA in defending our nation.

Roy Azevedo (01:26):

I'd also like to introduce our moderator for this panel David Ignatius. A fellow Massachusetts native, David is an award winning columnist for The Washington Post. And as worked as the Executive Editor of The international Herald Tribune, Assistant Managing Editor for business news at The Washington Post and a reporter for The Wall Street Journal. He's also the author of 10 novels, one of which was made into a movie. Thank you David, the floor is yours.

David Ignatius (02:05):

So General, it's a pleasure to be here with you, you're from an agency that used to be known as no such agency. And it's good to see you out and doing this kind of public event, thanks for doing it.

Gen. Paul Nakasone (02:18):

Thanks David.

David Ignatius (02:19):

So Russia has been a big concern of yours and your job from the beginning. And we have some interesting and different news about Russia in the last few days. The New York times reports this morning that CIA Director Burns is in Moscow, that he's talking with the Russians about possible new areas of discussion and cooperation. We have strategic stability talks that are going on between the US and Russia. I wrote the other week about a surprising development, a joint cybersecurity resolution at the United nations that was submitted by the US and Russia. I want to ask you whether from your standpoint as NSA Director and CYBERCOM commander, you're seeing any evidence of a different environment. And specifically, the area where President Biden has talked with President Putin and asked him to help namely ransomware attacks by groups, operating from Russia, whether you're seeing anything different from your perspective.

Gen. Paul Nakasone (03:30):

So David, first of all thanks and thanks to Aspen. It is truly nice to be back in the company of people. For... Yeah I agree. As we think about having a conference and actually being able to face to face it is so refreshing. Before I get to your first question, let me just talk a little bit. And I was thinking about this as I was coming down today. What's changed in really the almost, three and a half years that I've been in-charge of both the NSA and Cyber Command. So first of all, I think if you're going to talk about our agency at NSA, one of the things that's significantly different is the fact that it is a much more upfront, transparent engaging with the public focused on cybersecurity agency than ever before. On the CYBERCOM side, I would say is what I've seen over the past three and a half years is a growing capacity and capability in a number of different actions and a number of different capabilities that we've been able to bring in support of the defense of the nation. I'm very, very proud of that, but what hasn't changed over the past three and a half years, I think the first thing is; one, the importance of people.

Gen. Paul Nakasone (04:38):

Our number one strength at our agency and our man is our talent. No doubt about it. And the second thing David, to get to your question is there are still adversaries that are operating every single day in this space. The chairman really just talked about strategic competition. And this was with a number of different adversaries. Strategic competition is alive and well in cyberspace, and we're doing it every single day with Persistent Engagement. And, and I think the last point in terms of while I'll leave the policy pieces to our policy folks certainly we are obviously very, very vigilant. We are very, very prepared, well trained and I think very anticipatory of obviously the work that's being done on the political and the diplomatic front to get to a better resolution here.

David Ignatius (05:28):

Just to press on this question of ransomware attacks. I asked your government colleague, Jen Easterly, who's the head of CISA at the Department of Homeland Security, a month or so ago, if she'd seen or was aware of any Russian action in response to President Biden's request for help in dealing with these ransomware attacks. And she said, flatly, "No, I haven't." Would you say the same thing?

Gen. Paul Nakasone (05:56):

So I think it's too early to tell that's what I would say. And my good friend Jen is I think answering for a moment in time. And what I would say is let's let this play out, right? I mean, there's engagement going on again in a realm that it's outside of what I do, but I would say that it's too early to tell.

David Ignatius (06:15):

So to ask one more detailed question in the news, and I literally mean in the news, it just posted about a half hour ago. My colleagues at The Washington Post Ellen Nakashima, who covers your agency, very carefully and well. And Dalton Bennett just posted this story saying that Cyber Command last month conducted an operation against the ransomware group REvil. In which you were able to divert traffic that was heading to their servers. They went, "Whoa, what's happening?" Looked at their servers and realized that not simply because of Cyber Command operations, but others, that they had been compromised and shut down their operations, according to this story. The story says that Cyber Command wouldn't comment. And I don't think I'm likely to get you to go beyond that, but-

Gen. Paul Nakasone (07:11):

So you're going to ask the Commander Cyber Command?

David Ignatius (07:15):

But I want to ask in general, we're in a world where it is useful for the world, our adversaries and our friends, too, to understand the capabilities that we have. So without asking you about this specific case, talk a little bit about what you're able to do in this forward deployed mode that you've talked about. In dealing with groups like this that are creating such mischief havoc in the private sector.

Gen. Paul Nakasone (07:44):

Yeah. If you were to ask me this question a year ago, I probably would've said something along the lines of, "Ransomware, that's criminal actions that's handled by someone else." But what have we seen over the past year? We have seen adversaries use implants, adversaries use zero day vulnerabilities. Vulnerabilities that companies never ever see and are able to gain access. And then we've seen ransomware most vividly in the attack on our pipeline on the East Coast. So one of the things that we have done at both the agency and the command is we've conducted a search. And when you say, "Hey, so what is that about?" It's, we bring our best people together, David. I mean, the really good thinkers of how do you get after folks that are doing this? How do you get after the capabilities that they're producing?

Gen. Paul Nakasone (08:32):

How do you get after the flow of money? Those are all things that we have done over the past really three months. And while I won't comment on specific operations, I would say that we've made a lot of progress and I'm pleased with the progress that we made and we've got a lot more to do, but this is broader than just NSA and Cyber Command. This is working with Jen Easterly and great folks at CISA. This is working with, Chris Wray and the FBI, and specifically it's working with the private sector. And that's why this is an important piece of... And I hope we get to this, the public private mix that we have really realized we've got to do even more than we've done in the past.

David Ignatius (09:11):

So I want to ask you about one interesting feature of your job, which is that you wear two hats. You had head a normally civilian agency, The National Security Agency, and you head Cyber Command, the military command center for operations. When I've visited Fort Meade as a journalist I've been struck by this anomalous workforce. You walk down the halls and you see people in uniform who are sure, military people, and then you see people in black t-shirts and sometimes ponytails and ear piercings. And, those are part of your NSA workforce. And I want to ask you about managing a workforce like that. And then ask you to comment on the question that people raised for a decade. Which is whether it really makes sense long term to have those two quite different under the same net.

Gen. Paul Nakasone (10:12):

So first of all, I think you would say that coming to our agency in command is a reflection of our nation, right? I mean, we have a great demographic there. You do hit on a point that, we have people that look like me dressed like me have haircuts like me, and we have folks that don't look like me and can't cut like me, and that's perfectly fine. But what's the commonality that really kind of binds these folks together. Well, as one of my seniors at NSA once told me, he said, "I worked in the private sector for 40 years and I was just shocked when I first got to NSA and the first thing that they did is they asked me to swear an oath to the constitution." So that's the commonality that we all have. We all swear the oath to the constitution, protect and to defend.

Gen. Paul Nakasone (10:58):

The second pieces is that these are folks by nature that like to get after really hard problems. And we've got lots of hard problems and guess what? We've got incredible technology and incredible talent and we're all resourced and being able to solve these really difficult challenges like ransomware and election security and what our adversaries are to in cyberspace. These are folks that want to do that, and that's the whole focus of what they want to do no matter what they wear or what they look like. You asked me about the dual hat. I've had three and a half years leading both organizations. And I think I would just come back and say a couple things. First of all, at the end of the day, this is a decision that I don't make as a decision that are made by our policy makers.

Gen. Paul Nakasone (11:38):

But here's what I would share with you. Having led the organizations for three and a half years. What are we seeing in cyberspace today? We're seeing our adversaries operating at a scope scale and sophistication that's different. We're seeing adversaries that can morph quickly to do things that ransomware, and zero day attacks, and use bots very, very ingeniously to get after end states. And we're seeing the focus of not only nation states, but proxies and other criminals that are operating in the cyber space. The one commonality that I think is so important to have someone lead both organizations, is that you have to operate in cyberspace with three things, speed, agility and unity of effort. What's my proof for that? My proof for that now is successful election defenses in 2018 and 2020. The ability to have to ransomware the ability to take on unique challenges that the nation faces here. I think that's done with those three things. And in my experience again, is that, that's enabled by one person leading both organizations.

David Ignatius (12:46):

One criticism of that argument that the dual hat approach makes sense came after the SolarWinds hack devastating in its way. Identified as being conducted by the Russian intelligence service the SVR. A cyber commentator wrote on the blog of the Council on Foreign Relations. "The NSA support to Cyber Commands, operational requirements could have inadvertently contributed to the intelligence failure of not anticipating or uncovering the SolarWinds incident. And the argument, as I understand, it was you quite understandably are focused, outward. You're focused on foreign threats, and our adversaries are now able to appear to be operating from inside the United States. And that's part of why SolarWinds was so hard to find. And so devastating. I'm just wondering General as you reflect on that, whether there's any truth to that concern criticism and how you deal with it. I mean, our adversaries may not look like they're out in foreign networks in the future, but if you're focused there that may limit our ability to respond.

Gen. Paul Nakasone (14:08):

David, I think that is a really good commentary to talk about, again, the agility of our adversaries. We begin with the authorities of NSA and Cyber Command. They are outside the United States for very good reasons. We don't operate within the boundaries of the United States. The second piece though, I would say is that this is why it's so important for the partnership between public and private to continue to evolve. Let's talk about SolarWinds. A couple days before Thanksgiving in 2020 Kevin Mandia, the CEO of Mandiant came to NSA and said, "Hey, I think we have a problem here". We've talked about this public. We've shared that at his conference just the incredible foresight that he had to come to our agency. He came to our agency because he knew that we understood what goes out in foreign space.

Gen. Paul Nakasone (15:01):

So we understand the technical capabilities that we have, and he knew that he had a problem. This is the type of public private partnership that is so important. This is what I think, Jen Easterling is driving to and Joint Cyber Defense Collaborative JCDC Initiative. I think that's what we all want to do collectively, but again, let's come back to SolarWinds. Having run NSA for three and a half years, I would tell you the most damaging thing is to have a successful operation be uncovered. Now, while we didn't get to the theft here with regards to SolarWinds, we were able to expose this, and that's really great credit to Kevin Mandia and the folks that had worked it so hard across it. So this is a vector that is not going to be able to use by our adversary. And I think this is an example of the partnership that's so important.

David Ignatius (15:49):

So you've talked about public and private partnerships there is a way in which the NSA and even Cyber Command are now more transparent to companies in the US. When you have information about malware about dangerous vulnerabilities you're finding ways to share it. If you could talk about that and tell us where you want to take that connection with private business, private individuals in the US. GCHQ, your British counterpart now has a cybersecurity center that's extraordinarily outward facing and reaching. Do you want to be in that similar position?

Gen. Paul Nakasone (16:34):

So I think to answer that is just to kind of understand where we were and where we've been over the past couple years. In 2019, we re-stood up a cybersecurity directive. That's one of our two missions at NSA. And when I got there, that was one of the areas I said, "Hey, we need to change this because we need to be able to have one person in charge, focused resourced being able to do that. In 2010 was really our first big decision when we said, "Hey, we're going to publicly take credit for a significant vulnerability in the windows 10 software." So you'd say, "Well, how hard a decision was that?" It wasn't that hard a decision, but I would tell you, that's not necessarily the culture and the ethos that our agency had operated under for a number of years. And so I think that's a big change for us in saying that there's a vulnerability.

Gen. Paul Nakasone (17:18):

We substantiate the vulnerability. And I think that's important because when people look to The National Security Agency, I think there's a stamp on immature that says, "Hey, these guys are really good at what they're doing." And so when they release a product with CISA or FBI saying, "Hey, here are the 25 top vulnerability that the Chinese are using." People take notice. if you're a system administrator out there and you're trying to figure out what do you need to patch? Well, if NSA says, this is the most vulnerable thing, we probably should do that.

Gen. Paul Nakasone (17:46):

That's one aspect of it, but there are other aspects of the public-private partnership. At NSA I'm thrilled about the work that is being done by a number of different partners with us. Our Centers for Academic Excellence, the work with the National Cryptologic Foundation that has been established now for us to be able to go after talent and for a broader range of cybersecurity elements, an unclassified cybersecurity center that we've stood up side, the gates of NSA and for Cyber Command, it's the same way. An ability for us to do unclassified work in a facility called DreamPort in Columbia, Maryland.

Gen. Paul Nakasone (18:18):

These are all examples of what's being done. We're I'd like it to go. So we are very, very focused on national security systems. That's we're authorized to look. We're also very, very dependent upon the defense industrial base. That's where we want to go. And, and most importantly I wan to be the premier partner for folks like Chris Wray and Jen Easterly and the private sector when they need assistance.

David Ignatius (18:44):

Let me ask you a maybe unlikely question, but as we look at the cyber landscape, there is a huge difference from 10 years ago. Certainly from the four years of the Trump administration in that there is an absolutely emphatic stress on this issue. And there are lots of new people in prominent positions. I think of Anne Neuberger, who used to be your colleague at NSA, who's now in the White House in the National Security Council, big portfolio on cybersecurity. Chris Inglis, another former colleague of yours is the National Cyber Director, Jen Easterly heads CISA, which has oversight of a lot of these activities. Then you've got individual activities by the FBI, other agencies. The management consultant looked at that organization chart. He, or she would worry that there are too many boxes there and that the lines are hard to follow. And I just want to ask whether we need to think more about how to coordinate that so that we don't end up with what we've seen and national security can be still quite yeah.

Gen. Paul Nakasone (20:06):

I think David, I begin with... You highlight, I think some great choices. I obviously Anne and Chris and Jen are folks that we know well at our agency. They've contributed tremendously at our agency in, in positions there. And they're the right folks to lead these organizations. But I think to your question, I mean, we organize within our government based upon our ideals. What we believe in what the Constitution's says. And so when you take a look at that, you have a number of different players. I think it does make sense, right? I mean, it makes sense to one organization that is looking outside the United States, like the Department of Defense and the intelligence community, another organization that's focused within the United States that comports with how we believe government should be run.

Gen. Paul Nakasone (20:50):

But I think to your point is our challenge as leaders is, so how do you stitch that together? What makes that look effective? And I think you could begin with election security and say, "Hey, here's an example. Or here's something where you've gone across a number of different agencies and in the past couple of election, you seem to have had some success." And so I think that, that's a really good starting point as we take a look at how does this broadly get to our ability to defend the nation in cyberspace.

David Ignatius (21:19):

Let's talk a little bit more about your mission in countering foreign attempts to in interfere with our elections. That's been a very visible NSA, Cyber Command responsibility. We were all focused on it after the 2016 election. You were quite open in talking about this Russia small group, as you called it at NSA and Cyber Command that was working in the 2018 midterm elections that obviously continued in the 2020 elections. Give us an update on those activities. And if you would give us lessons learned, you've been now through three election cycles. You've learned a lot about our vulnerabilities what to do to defend ourselves what the future threats are going to be in this space of guarding the security of our elections.

Gen. Paul Nakasone (22:20):

So to understand, I think the future, you have to go back to 18 where I think it's really the seminal event where we said, "Okay we're going to come together as both a command and the agency, but it's more broadly than that. It was a command and agency. It was CISA, it was FBI. How do we work together? One threat primarily there. We worked it very, very hard. We had success there and I think out of 18, we learned a couple things. We learned the fact that we have to have a broader set of partners. We came out of the election in 18 saying, "This is not going be just one adversary in the future. And so we've got to be able to scale. And the third thing I think we said is, "Hey, there are other partners here that we haven't had an opportunity to bring into the fold."

Gen. Paul Nakasone (23:00):

So 20 what's the difference in 20 more actors in terms of adversaries, trying to influence our election, a broader set of partnerships. So, the ability to work with a national guard, the ability to work with academia, the ability to work with select international partners and the ability to work with the private sector that I think that CISA and FBI did so well in 2020. What does it mean for the future? The future, I think is really composed of really three things that we're going to have to do. So first of all, internally to our command and our agency, we have to generate insights.

Gen. Paul Nakasone (23:35):

So we have to go into elections knowing the adversaries better than they know themselves. The second thing is we have to figure out how to share information. Share information rapidly. I meaning that we learned in 18 is that we could really help the bureau. If we could provide information to them that they could pass on rapidly to social media companies, which they did so effectively. And the last thing is that, "Hey, we, we've got to be able to somehow impact adversaries that don't get the message. We're going to have to impose costs in them. And so that's a little bit of the election landscape, not only now, but I think into the future

David Ignatius (24:13):

In terms of the imposed costs, part of that, what has been reported in the news media is that in 2018 and presumably subsequently, some of these malign actors Russia is at the top of the list in terms of election interference. People who were seeking to interfere in our elections were confronted by the cyber presence of cyber command through its partners. There have been published reports about how you you're forward deployment as you working with services in Eastern Europe who were familiar with Russian networks. And that you were able to make them feel some pain. Is that a good way to put it?

Gen. Paul Nakasone (25:04):

So I guess what I would say David it is that in 2018 we were really putting, the final touches on what we call Persistent Engagement. And Persistent Engagement is based upon the department strategy of defend forward. That is how do you operate outside the United States to do two things, one enable partners and two to act. And so, to give you an example in not only 2018, but 2020, we sent over 10 hunt forward teams to different countries. "Okay? And, what is a hunt forward team?" It's a group of really good cyber soldiers and civilians that goes to a country at their behest to hunt on down the networks. And what are we hunting for? We're hunting for malware or we're hunting for trade craft, we're hunting for any of indication that our adversaries might be utilizing, that we can then expose again, when you expose tools.

Gen. Paul Nakasone (25:52):

When we share that information with the private sector, again, back to the point of public private partnerships. It gives that inoculation for a lot of networks against an adversary that thinks they have a tool. We have conducted operations. I think that, that's been well established and talked about by the government in 2018. And while I won't go into the further depths of that, I think the important thing to emphasize here is that we have a capability. We have obviously a process upon which we utilize that capability and we have really well trained people.

David Ignatius (26:27):

I use the phrase feel some pain. Is that an accurate description of what those capabilities can do?

Gen. Paul Nakasone (26:35):

So I think you'd have to ask our adversaries if they felt some pain.

David Ignatius (26:40):

We'll have them for the next next Aspen Security Forum absolutely. So you mentioned Persistent Engagement. And one of the really things you did when you became Cyber Command Commander and head the NSA was to give a lengthy interview to joint forces quarterly. Not on most of daily reading lists, but It was a detailed discussion of your doctrine. And you talked about Persistent Engagement. And my takeaway was that you were saying the United States now is in a constant, low level, state of cyber conflict with its adversaries. That we should no longer think of conflict in this domain as an on, off switch. You're either at war or you're not, but it's a rear stat. And that the rear stat is kind of permanently set at about two. In this Persistent Engagement world. And I want to ask whether as you've gone down the road you would expand on that idea of Persistent Engagement. And am I describing that kind of constant state of conflict that, sliding rear started about to right?, And I've worried personally looking at the news that real stat's going up to three or four. So I'm curious about that too.

Gen. Paul Nakasone (28:10):

So I think I would change the word conflict to competition. I think we're in competition every day, and I think that's why the chairman's talk about strategic competition in a number of different domains is so important. That's what we're in, in cyberspace. What our adversaries trying to do. They're trying to steal intellectual property. They're trying to interfere in our elections. They're trying to have other marked impacts on our diplomatic or our economic efforts. This is the world in which we operate. And so when I was trying to explain in 2018, what Persistent Engagement was, I again, I came back to two points. I said, we're going to enable our partners. And then we're going to act when authorized and think that was the difference in 2018. Given the fact that we had a new strategy that said, "Hey, we're going to operate outside the United States. And we're going to look for adversaries that might be trying to do us harm. And we're not going to just watch anymore." And I think that, that was a pretty big watershed event.

David Ignatius (29:02):

So in the military realm we like to think that deterrence operates. That we have such capabilities, that our adversaries will be deterred from actions that would harm us. As the whole premise, obviously of our nuclear deterrent. But there's been a lot of discussion about whether that model really applies to cyberspace. And certainly, we have all these capabilities. Your command, the NSA probably still best in the world. So you'd think that we'd be able to deter, but as you look at the rising number of attacks, you wonder, does deterrence work in this domain? So I want to put that to you directly, does the deterrence model work, or do we need to think about it in a slightly different way?

Gen. Paul Nakasone (29:56):

So I grew up in the deterrence world that you described, right? It was a nuclear deterrence world where it really was a binary yes or no. That that we understood that one nation had these capabilities when use those capabilities. And the other nation said, "Okay, I understand that." That's a different world than the world of cyberspace. I don't think that that's a model that comports, I do believe as Secretary Austin has talked about there is a model of deterrence that probably includes such things as integrating what we do with our partners. What we do in a multiple number of domains. So it's not just cyberspace that we're trying to influence our adversaries. It could be cyberspace on the ground, air, sea. And other ones that that we're trying to obviously get our adversaries to change their behavior.

Gen. Paul Nakasone (30:45):

I think thirdly is that there is a piece of deterrence that certainly works with regards to resilience and defense. That's so important that we have to be able to do. But I think broadly to your question, I think that we're still a learning organization. How the deterrence model is going to play out and how much of the competition space influences what adversaries are doing. We're still learning at this. And I think that there's a number of different efforts that are showing us that there are ways that we can improve it.

David Ignatius (31:15):

What do you think of the effort the most prominent advocate really is the President of Microsoft, Brad Smith for international rules of the road, a kind of Geneva Convention, he likes to say for cybersecurity. That's something that the US Government has often been reluctant about because it might limit our own ability to take actions and we have such extraordinary capabilities. What do you think about that idea today and how it would affect the world you live in?

Gen. Paul Nakasone (31:55):

So Brad and I have had this conversation, in some forms outside of out of Aspen. And one of the things that I continue to say on this is that obviously that's a policy element that the policy makers work through and will decide on it. What's my responsibility? My responsibility is provide a series of options to the President and provide insights to the Secretary of Defense and the Director of National Intelligence in terms of what's going on. So again, I'll leave that policy piece, but I think what I need to be able to do is to make sure that our adversaries understand that both in terms of US Cyber Command, The National Security Agency, we have the capabilities upon which, if the President so decides and authorizes that we can use.

David Ignatius (32:37):

So you wouldn't. This question of whether rules of the road would be too restrictive for the United States. Is there a view you have on that, that you're willing to share?

Gen. Paul Nakasone (32:51):

No.

David Ignatius (32:51):

Okay. So you've talked a number of times in our conversation about partners and partnerships. And you operate in a world where, the most exclusive security partnership ever known as Five Eyes. Is just the combination of the closest allies that we've had deep levels of trust and sharing. And as you talk about

partners in this world of increasingly difficult threats, is it sensible, do you think to expand not Five Eyes per se, but expand that extraordinary level of trust and cooperation to other trusted partners. So that we have a somewhat broader and more robust ability to operate in the world.

Gen. Paul Nakasone (33:53):

I think that partnerships, and certainly the secretary and the chairman have talked about this. Partnerships are really the lifeblood that makes us so different than our adversaries. We have enjoyed a historic partnership with the Five Eyes as you've noted there. But there are other partnerships that certainly that we will continue to work between like-minded nations. I would anticipate that new challenges to our nation are going to require us to look at forming other partnerships. But I think, rightfully so I think that the Five Eyes will continue, and I think that it will continue very strongly. And I think that we will build other partnerships based upon the circumstances and the missions that we're going to have to look at as a nation.

David Ignatius (34:40):

The Quad, which is the informal partnership, not a security Alliance but a partnership between the US, Australia, Japan, and India is big effort by this administration. There's a new trade and technology council with the European union and each of those formats. There's been quite a lot of discussion of cybersecurity issues. And I'm wondering whether you either in your NSA role or in your Cyber Command role have participated in those, and whether you'd envision somewhat more participation in those kinds of forums that are about joint security but outside the Five Eyes framework.

Gen. Paul Nakasone (35:26):

David, it's interesting because if you think about any type of partnership that our nation is trying to engender. What's commonality that that nations can seek? So one of the commonalities is certainly cybersecurity. So in general, I would say this is one of those areas that I would anticipate that our nation wants to pursue with other like-minded nations. I am intrigued by a number of the different guide. I've just seen the Chief of Naval Operations off the coast of India working with the Indian Navy. I think that again, to the changing dynamics of our security environment, you have to believe that there are going to be just unique partnerships that come from that. And again, I come back to is if you're looking for a commonality, most nations say, "I'd like to operate with you in cybersecurity."

David Ignatius (36:14):

Mm-hmm (affirmative) And you'd be open to that with than rules that are set by policy.

Gen. Paul Nakasone (36:19):

Well certainly, I mean I think that one of the strengths of both the command and the agency is that, we've been able to work with a number of different partners. And that's indicative of what we're going to do in the future as well.

David Ignatius (36:31):

Let me ask one of the hardest questions I'm sure. Which is the security of your operations. NSA has faced some insider threats from employees. The Edward Snowden case, wasn't exclusively NSA, but it sure had an effect on you. There have been other cases since then, and of employees who took an awful lot of very classified material, it seems out of their workspace. And there's been a continuing question

among people who follow intelligence about whether there's a deeper counterintelligence problem for you at the NSA and at Cyber Command. That there's somebody inside who's been feeding information and is still not detected. So I know counterintelligence is a very sensitive issue, but I want to ask you both on the insider threat level and the broader counterintelligence level whether you feel you got a handle on the risks to NSA and Cyber Command.

Gen. Paul Nakasone (37:45):

I have tremendous confidence in the folks that work at our command and our agency that look at counterintelligence. I would tell you that we have not been still, we have not been static in terms of looking at what our vulnerabilities are. I'm sure that's true of every director they think about this. But, I think in general, I would say that we are in a much better spot today. But it's not a spot that we will ever rest on.

David Ignatius (38:12):

So I want to ask you one last question, then we're going to turn to our Aspen Young Leaders Group for couple of questions. You have been at NSA I believe for four tours, you've been a Cyber commander for many years now. And you have a body of experience that's probably unmatched. And so I going to ask you, if you would just share with this audience the things you'd like to do going forward. You talked about a lot of the initiatives you made, the things that you've gotten done. What is still on your to-do list that you might be willing to share with us that you think would make these two agencies stronger?

Gen. Paul Nakasone (39:06):

The number one thing on my to-do list is talent. Even after as many times as I've been at NSA and the experiences I've been at Cyber Command. It comes down to the equation of who has the best talent? I'm convinced to that. I mean, I've seen it. I've seen the benefits and we certainly have been beneficiary for as of tomorrow 69 years of great talent at our agency. So I'm always thinking about that. What can we do more of, what can we do more to recruit? What can we do more to retain? What can we do more to have our folks rejoin our agency when they leave it? I think the world is changing. And so we have to change just as rapidly to be able to be competitive and attractive.

Gen. Paul Nakasone (39:49):

And in this mix of talent. I think the second piece is over the coming months, I think that clearly cybersecurity is going to be central to the national security of our nation. And I think that, that's an area across both the command and the agency. I hope to leave my mark. We were able to stand up a new directorate. We have outreaches to the private sector. We're working very effectively, I think, with our government partners. But there's more to do. And I think the last piece I would say in just moving forward is really is just continuing to maintain that state of readiness that we've had for so many years that the agency and the command. That our nation's going to face different challenges in the future. Perhaps not the challenges that we think today. And so how are we agile enough to be able to get those challenges, that's with a mindset and a culture and an ethos that, I think that we've made tremendous progress at the agency and command on.

David Ignatius (40:50):

So you refer to young talent and we have some here in our Aspen Security Forum Rising Leaders. I see a hand up from a rising leader. Let me recognize you for a question.

Erica Lee (41:03):

Hi General Nakasone thanks for being here today. My name is Erica Lee. And my question for you is, do you believe that the NSA and CYBERCOM are adequately or appropriately resourced money personnel, technology, and capability development for the speed scale and scope of not only great power competition, but to also combat malicious non-state cyber actors?

Gen. Paul Nakasone (41:26):

So, Erica, a really good question. And you can, well imagine anyone that leads two organizations that they would never say they have enough resources. I would always like more resources. But I would tell you that we are very well resourced across both the command and the agency. Part of what we have to do now is the resources that are given to us. How do we effectively apply them to the challenges that you just noted there? This is not only resource. This is how is the mindset? How is the culture upon which we're going to operate. Those are all things that we're very, very focused on. So thanks a lot for the question.

David Ignatius (42:02):

Do we have another question from one of our rising leaders?

Helen Toner (42:11):

Thank you, General Nakasone so much. My name is Helen Toner. I work at the Center for Security and Emerging Technology at Georgetown. My question is about China and some of the intrusions that they have managed to pull off over the past few years. On the one hand, people look at things like the OPM hack, Equifax and so on, and they say, "Well, China looks like it's gathering lots of data on American citizens, American officials, and putting all together in ways that it will be able to use." On the other hand, we know that data fusion is incredibly challenging and using any data scientist knows that 95% of the work in solving any problem is cleaning and structuring the data. So I'd love to hear your take on the extent to which you think China does have some kind of underlying plan or underlying ability to combine what they're gaining from these different intrusions. Versus the extent to which you think they're fairly separate incidents. Thank you.

Gen. Paul Nakasone (43:00):

So Kelly, first of all, thanks for the question. And I think you hit on the great geopolitical change of what our generation and your generation is going to have to deal with which is China. This is unlike anything I've ever seen before. This is not the Soviet Union a problem which I grew up in. This is a nation state that has a dis different risk calculus. That's impacting us economically diplomatically, militarily, and informationaly. In terms of their intent for the data that they continue to steal and utilize. I would say that we have to be just vigilant in terms of one, how do we get to a higher level of cybersecurity so we prevent this type of work? But two we should not underestimate, the capabilities of our adversaries. And that's something that, I've probably learned over three decades in service to the nation. So thank you very much and good luck.

David Ignatius (43:48):

So we've come to the end of our allotted period. It's 10 30. Just want to thank I'm sure. On behalf of everybody General Nakasone for coming here to be with us. It's great when the representative of America's basically most secret activities comes and talks to a group like this. Thanks a lot for doing this.

Gen. Paul Nakasone (44:09):
Thanks, David it's always good to see you. Will you come back?

David Ignatius (44:10):
With pleasure.

Gen. Paul Nakasone (44:10):
Thank you. Excuse me.