THE ASPEN INSTITUTE

ASPEN SECURITY FORUM

Countering Threats Old and New

Greenwald Pavilion
Aspen, Colorado

Saturday, July 21, 2018

Dan Porterfield: Hello, my name is Dan Porterfield and I'm the president and CEO of the Aspen Institute. It's a great pleasure to be able to welcome all of you to another scintillating session of the Aspen Security Forum. Please join me in thanking all of who have made this remarkable forum possible and I'm thinking in particular of my Aspen Institute colleagues Clark Ervin, Rob Thomas, Elliott [Gercin 00:00:27] and their team, along with the dozens of colleagues who put up tents and made meals and cleaned buildings and transporting travelers from all around the country to get here. Thank you to everybody who made this possible.

It is wonderful to have commander of US cyber command and national security director General Paul Nakasone here and the BBC's Gordon Corera for a discussion on countering old threats and new. Needless to say, these last few days have been quite a convening. After our opening session with FBI director Christopher Ray on Wednesday night, I needed to travel to Washington DC for some meetings and I just got back late last night. Well, while I was in DC, Associate Attorney General Rod Rosenstein, national intelligence director Dan Coats, both made honest unvarnished comments about the destructive behaviors of Russia in relation to our national security, elections, internal unity, and our standing in the world, even, and it was like parallel universes standing in Washington DC and reading the media coming from my home here in Aspen, Colorado.

Washington DC right now to me stands paralyzed like we've never seen it before while Vladimir Putin and his people are making pronouncements about a new bilateral agenda that we're all gonna learn about some day. Much of DC seems to have laryngitis and maybe amnesia waiting for the next shoe to drop. Then, conversely, there's Aspen, Colorado. Admittedly, not normally thought of as the epicenter of hard-nosed fact-based realism. However, it's clear that over the past four days, there has been no more concentrated, candid, principled, non-partisan, and patriotic commentary on the nature of US/Russia relationship and, more broadly, all of our security threats than the Aspen Institute's on the record convening right here. It has been extraordinary.

I say on the record with intentional emphasis and real pride. I'd like to express our collective gratitude to the government officials who joined us a the Aspen Security Forum to talk and think together and answer the uncensored questions of skilled reporters and moderators who prepare diligently for the interviews. Government accountability and freedom of the press are the American way in good times and bad. And, it's quite the opposite in Putin's Russia. There, power doesn't open itself up to media inquiries. Power avoids questions, smears reporters, locks them up, or worse as we know from the 2006 assassination of Anna Politkovsaya and dozens since then documented by the committee to protect journalists and others.

Our tradition is different and our systems are not equivalent. They weren't equivalent when I was Alexander [inaudible 00:03:50], and Lech Walesa, and

Vaclav Havel were working as dissidents under death threats. They weren't equivalent when President Reagan called on Mr. Gorbachev to tear down that wall. They aren't equivalent today in an era when cyber technologies allow Russia and, yes, other countries to steal, stalk, spy, attack our processes of elections and incite civil discord within our population. It is not equivalent and this forum has laid that out again and again over these past few days. We can't turn a blind eye to the real and complex dangers of the modern world. September 11th taught us that. This forum has reminded us of that and that's why it's so valuable.

Three big reasons. First, the Aspen Security Forum helps us confront the fact that we must see and stop the risks that threaten our nation's security and our way of life. We must confront those risks in real ways. Second, this forum allows us to practice and model the democratic virtues that bind us to one another as Americans and the great democratic nations who are our longstanding allies. Third, this forum, working at the highest level of security expertise and commitment to our Constitution, allows us to join hands not as Republicans or Democrats or Independents, but as Americans. Thank you all for being here. It's been a great few days. Thank you very much. Now it's my pleasure to welcome to the podium, Clark Ervin, the chairman of the Aspen Security Forum. Clark.

Clark Ervin: Thank you so much, Dan.

Dan Porterfield: Thank you.

Clark Ervin: Well, everyone, you've heard enough from me over the course of these few days and thank you, Dan, for those powerful words that I think set the stage perfectly for tonight's conclusion session. To introduce tonight's concluding session, I'm pleased to introduce Mark Pasquale who's the vice president and general manager of special programs at Lockheed Martin Space. Mark.

Mark Pasquale: Thank you, Clark. It's my distinct honor to introduce our next session countering threats old and new. Our speaker tonight, General Paul Nakasone, is a tremendous leader and seasoned officer charged with confronting some of the most significant national security challenges facing our country today. His military roots run deep as his father as retired Army Colonel with military intelligence background. General Nakasone's noteworthy career of service spans from employment of classic hard power during deployments abroad to the burgeoning and ill-defined combat domain of cyberspace.

As both the director of the National Security Agency and the commander of the United States Cyber Command, he's not only responsible for a vital component of the intelligence community, but for shaping the future of US military capability and resolve in the evolving virtual world. With his impressive background, there's no better person to wear both indispensable hats. We're also privileged to have as our moderator tonight Mr. Gordon Corera. Gordon joined the BBC in 1997 and was selected as a BBC News security corespondent

in 2004 focusing on terrorism, cyber security, and intelligence matters. He's also recently published a book called Cyber Spies. Before us is a fantastic opportunity to hear from a leader of those that safeguard our nation every day, so please join me in welcoming Gordon Corera and General Nakasone.

Gordon Corera: Thank you very much. Thank you all for being here. Thank you for join us with the last session of what's been a fantastic forum and it's a great privilege to be able to moderate this. Now, as we just heard, General Nakasone wears two hats, not literally, because that would be a bit weird, but two hats as director NSA and the head of cyber command, so he's here really primarily talking in the cyber command capacity and I think it's a chance to explore what cyber command does, how it works, the threats that are out there in cyberspace, the challenges posed by new technology, as well, but first of all, I just wanted to learn a bit more about you because you've been in this post only for a couple of months, but you grew up in the digital age, didn't you? Your career has been focused in a way on this cyber issue perhaps more than others in the past. Did you start off as a kid being interested in computers? Did you join the military thinking you were gonna do cyber? How did you end up here?

Paul Nakasone: Gordon, first of all, thank you very much. I'd like to first of all thank the Aspen Security Forum for putting this on today obviously to all of you who have stayed throughout the entire day for this last piece of it and I must admit that I feel like the person that's at the party that didn't get the invite in terms of what you should wear. But nonetheless, let me begin. Before I talk about myself, let me talk about US cyber command because nine years ago, I was at the National Security Agency working for the director named Keith Alexander and he said, "I've got this idea."

Now, for those of you that know Keith Alexander, that's either you run or you hide and I missed both opportunities. Over a period of a year, myself and three other officers put together this concept of cyber command, brought it from the ground up, designed it, and in 2010, it started. For myself, I would tell you I have watched the birth, really to steal a term from a great Secretary of State present at the creation, have seen the development of US cyber command throughout the years, and I would tell you that we have built a force. We have trained that forced. We've equipped that force. We've employed that force. It's a well-prepared force. It's a ready force. It's a learning force.

In terms of my own experiences as you asked, I would trace it really back to 2007 when I landed at the National Security Agency pretty sure that my career was done and they told me, "Hey, you're gonna be in charge of support to military operations," and so over the period of three years, I really learned a lot about our agency in terms of what the could do for forward deployed forces and I would tell you it was incredible. The technologies that we talk about today: cloud technology, AI, big data, we were doing that in 2008 and 2009 in places like Iraq and Afghanistan and if you read the memoirs of some of the

commanders on the ground, you see how impactful a small group of agency people forward deployed had on the eventual outcome of the search.

I transition from there to command of our Cyber National Mission Force and I've also had the opportunity to command most recently Army Cyber Command where I was also commander of our joint task force Aries which you may know as the element that does offensive cyber operations against ISIS, so through that, I guess, over the past 10 years, I've seen really the development of a very, very capable and, as I said, ready force.

Gordon Corera: What did you learn from those operations against ISIS?

Paul Nakasone: What I learned is I think the first this is that it really gets down to a very, very small group of people. We talk about the technology all the time. We found the right leader for JTF Aries, a one star that is currently now with the command. We found the right people across the services and we put together very, very small teams. We worked with our partners. I think many of you have read what GCHQ has done and I would also tell you that we had development that was paired with our operators so we could actually develop our capabilities on the fly. It was a very, very dynamic environment.

Gordon Corera: And this is going after ISIS, going after its cyber operations, its ability to communicate?

Paul Nakasone: This is going after in support of forces forward in northern Iraq, in Syria, in other places around the world, ISIS, and it's also not on the ground, but it's also as they move to a virtual presence. That's a very, very difficult concept that you work through as time goes by.

Gordon Corera: Now, as you took over in May, Cyber Command became a unified combat and command. What does that mean in practice?

Paul Nakasone: It means in practice that there are 10 unified command across our force. The joint force organizes under combatant commands to do our war fighting, so it provides a very, very streamlined command from the president to the Secretary of Defense to the combatant commander. It gives increased resources and I would tell you it also gives a signal to not only our nation, but to our allies and adversaries that cyberspace is an incredibly important domain upon which we operate.

Gordon Corera: Cyber Command now has 133 mission teams. What do the do?

Paul Nakasone: 133 mission teams. Each of the services, our force services are responsible for building these teams. They're offensive teams. They're defensive teams. They're support teams. They do everything from defensive work to ensure that our networks, our data, our weapons systems are protected to doing offensive operations against our adversaries as I described against ISIS and others.

Gordon Corera: Are they day by day? Are they battling adversaries in cyberspace trying to keep them off networks or trying to take them on? Is that the kind of thing that we're talking about or are they preparing plans for future operations? What's the balance?

Paul Nakasone: So yes. Lemme expound upon that a bit.

Gordon Corera: Thank you.

Paul Nakasone: This is an environment ... I think we should talk a little bit about cyberspace, right? Cyberspace is an environment upon which you have to be engaged every single day. You have to be engaged understanding what your adversaries are doing, so certainly in terms of what our defensive teams are doing, what we're doing to prepare and plan for future operations, that's all part of that and it's all very interesting to note that across those 133 teams, we took really some lessons learned from the stand up of special operations command. What did we learn from SOCOM? We learned the fact that there was power in having a joint standard that it wasn't just an Army team or a Navy team or an Air Force team. There was a joint standard so when a joint force commander like myself gets a team, the standard is the same and I think that's a very powerful lesson that we learned from SOCOM and one that's we've been able to put into practice every single day.

Gordon Corera: There's a phrase in your vision statement about continuous engagement. What's that mean?

Paul Nakasone: Again, this idea, and let me come back to our adversaries. I would tell you that what we've seen our adversaries do over a period of years is the fact the they operate below the threshold level of war so that they steal intellectual property. They still PII or information on personnel. They cause discord within our social ranks or attempt to undermine our elections all below the level of war and so this idea of how do you engage that force is something that I believe needs to be on a continual basis. It fits very, very closely to our national defense strategy that talks about strategic competition.

If you think about strategic competition and the idea of our adversaries every single day are looking upon which that they can have a campaign or a strategic outcome against us, I look at that in cyberspace as well, so one ability of our adversaries to take our intellectual property may not mean a lot, but over time, you see this is a campaign and over time this has a strategic impact. Over time this has perhaps a strategic impact on our nation's economy and our national security.

Gordon Corera: So it's about contesting that? Because people say cyberspace, the boundaries between war and peace are not the same as in regular military conflict. There's a kind of gray space in between in which things are happening all the time and you're engaged in that. Is that the idea?

Paul Nakasone: I do believe that. I think that there is an engagement every single day that either you're monitoring your force or you're imposing cost in that force or you're understanding what that force wants to do. That's really important.

Gordon Corera: Does that evolve, in terms of just defending ... You hear people talk about it's important not just to do goal line defense, in other words, not just to be the goalkeeper defending your networks against attacks coming at you, but a bit like in football, or as you might call it, soccer, going and attacking your opponent. Is that what it takes sometimes not just to be sitting back and trying to defend, but actually trying to get to them before and keep them off balance or to try and attack them before they attack you?

Paul Nakasone: This continuous engagement, I think you hit an important point. It's at one time playing offense, one time playing defense. It's the idea of what you might be doing in an adversary's network to learn what they are doing that might improve your own defenses. It's ensuring that what we may be doing against an adversary, we're protected against our defenses. It's also this idea that we want to have our forces to be able to enable our defensive capabilities and to act forward. Act outside the boundaries of the United States to understand what our adversaries are doing and being able to engage those adversaries and obviously being able to protect our networks, our data, and our weapon systems.

Gordon Corera: Let me ask you what might sound a simple question, but in cyberspace is a complicated one. What are you there to defend? Some of the talk already over the last few days has been government can't be expected to defend everything in cyberspace. There's all kinds of threats out there from non-state actors, hackers, but also you have other states targeting private companies. Where do the boundaries like between what you defend as the military, what the government defends and what you expect people to defend themselves?

Paul Nakasone: Great question. So my remit, what I'm tasked to do, is first of all to defend our Department of Defense networks. It's not only the networks. It's our data. It's our weapon systems. I think you know within the United States, the Department of Homeland Security has the responsibility for the defense of our critical infrastructure and so there's a partnership there. As we can enable or we are asked to assist, certainly that goes through a process and the Department of Defense would answer that request, but I think it's really what we've learned over time is that that partnership has to continue to grow, has to continue to get stronger, so while our focus, our authorities right now are within, clearly, the protection of our own networks within the Department of Defense. We are also an available force upon which, if the nation needs it, can be called on.

Gordon Corera: In other words where ... Because we've seen instances where you had, if you go back to 2014, you had the North Koreans targeting a private company, Sony. That would not typically be something you'd expect the military to be called in to defend, but in the future, can you imagine that kind of scenario of someone

saying, "This requires you to be involved in helping defend against this," and that would come from coordination with the Department of Homeland Security, would it?

Paul Nakasone: Certainly, and I guess I would take a step back and say at the end of the day, what does the Department of Defense do? It defends the nation, and so if called upon, then I would certainly imagine whatever scenario that you could draw, if called upon, our Department of Defense would answer that call.

Gordon Corera: Let's talk a bit about the threats which are out there in cyberspace. Let's start with the one that everyone's been talking about in this conference, Russia. How do you see the threat from Russia and what are you doing about the threat from Russia?

Paul Nakasone: I think many of you know, you may have read that [inaudible 00:20:01] Russia group-

PART 1 OF 3 ENDS [00:20:04]

Paul Nakasone: That I stood up a Russia group, Russia small group, the RSG. That is true. It's in line with what the intelligence community has really been doing since post 2016, 2017 upon which making sure that we understand in which we operate. That fits very, very clearly with the requirements and the direction I received from the Secretary and certainly our administration but also fits, in terms of how I look at problem sets, again coming back to my own experiences, I see small groups that come together that bring capabilities after an adversary.

In terms of how I look at the threats, again, coming back to this idea of strategic competition that we look at as a nation now certainly Russia, a near pure threat, great capabilities upon which we will certainly be called upon. And if called upon I think no doubt we will ensure that we act.

Gordon Corera: One of the things that's been striking over the last few years is the escalation and the proliferation of cyber attacks. So we've seen escalation in terms of countries being willing to go further than we'd seen before. Russia allegedly turning off a power plant in the Ukraine. We've seen proliferation, we've seen countries which previously weren't seen as having high end attack capability, kind of Iran, North Korea, carry out pretty sophisticated attacks. What worries you most? What are you seeing in terms of the threats coming next?

Paul Nakasone: So I would answer this in a couple of different scenarios as I've seen over the past really 10 years. We began the discussion of threats with the idea that our adversaries may be doing exploitation, or what we would consider spying, on our networks. And then that advanced to disruption. This is the whole denial of service attacks that we had seen from our adversaries. Then on the very, very high end the idea of destruction and what you had indicated with Sony Pictures America.

But I think there's also been some other trends that we should recognize. In the spring of 2011, in April of 2011, Arab Spring. We looked at this in terms of what I would say myself included as wow this is an indicator of how powerful a free and open Internet can be in the world, and we looked at this from that lens. But I would also say that our adversaries looked at it from a completely different lens, an existential threat to their existence.

So what have you seen since then? I would say the weaponization of information. The idea of being able to control the populous with this information. And I think that's an incredibly important trend that we're starting to see.

And the other one, I would say, is certainly the idea of data and the importance of data, the stealing of data, the importance of being able to secure your data. This is all, I think, the trends that we've seen over the couple of years that I've certainly noticed.

Gordon Corera: Your focus is on cyber but it's striking how Russia in particular has integrated cyber with other forms of activity, what some people call hybrid warfare, in which they might be linking cyber attacks with unconventional warfare and troops going in under cover into the Ukraine or it might be hacking emails but then releasing them through social media, or ... Countering that kind of hybrid threat in which cyber is just one part of it that's a challenge isn't it? Because that requires the US government as well working across different agencies and departments as well. Do you think the US government is ready, is it equipped, should it be able to fight that kind of hybrid warfare? Either to defend it, or to be able to do it itself?

Paul Nakasone: So let me begin at more of a tactical level, 'cause I think the Secretary of the Army today in his talk indicated, I think, something very important. And that is we've recognized this importance of hybrid warfare within our army, within our Marine Corps on the ground. We've already started to take actions and started to train in places like the National Training Center that incorporates the idea of information warfare with a ground combat element.

I think that this is really instructive of how far that our thinking has come in terms of we have to have this capability within our tactical forces, certainly within our nation. This is an important piece of it that has to be a whole nation approach. And I do think our nation is capable of it. This is not something new. This is something that we've done previously. This is something that we have ... I certainly grew up with it during the cold war, have done very effectively. And I think we will do it again.

Gordon Corera: So it requires that whole of nation approach to deal with cyber and hybrid and these kind of new threats that we're facing?

Paul Nakasone: Most certainly.

Gordon Corera: There's a lot of talk about foreign presence on the critical national infrastructure. I know you said that was a Department of Homeland Security issue partly but in terms of dealing with it, is there a role for the military in deterrence in being able to say we are going to deter you from coming into our networks? And do you think there's been enough on that? Because I think in your confirmation hearing the question came up, has enough been done to deter Russia and other countries from carrying out these kind of cyber attacks in America? And you suggested it hadn't been. Are you looking at ways of actually trying to create that kind of deterrence?

Paul Nakasone: So I come back to the idea of persistently engaged. We should anticipate in this domain, within cyber space, that our adversaries will continue to penetrate, and try to penetrate such things as our critical infrastructure. What should we do about that? And I say I think it's both the idea of being vigilant about that, certainly. It's also the idea of being able to act forward in terms of understanding what your adversaries may be doing within their own networks. And then I think it's the idea of enabling the idea of what's the partnership that's most effective to ensure that the Department of Homeland Security is armed with, and has the information in both the capabilities upon which to deal with these type of threats.

Gordon Corera: But do you think there is a sense yet of how deterrence looks in the cyber age? 'Cause it doesn't look the same as nuclear deterrence does it? It doesn't look ... some people posit that you could have a kind of mutually assured destruction in which they're inside our critical national infrastructure, we're inside theirs, no one's gonna switch it off because they're too scared of the consequences.

That's one possible view of deterrence, that kind of nuclear style but do you think that's a realistic concept? 'Cause cyber is quite different from the nuclear world, isn't it? In terms of being able to attribute attacks, to know who's doing it, that can take time. It's different from a missile coming in.

Paul Nakasone: So certainly there is differences in terms of where we operate in cyber space. If you think about ... first of all lets begin with the idea of monopoly of power. In the nuclear realm certainly nations, or nation states, had the monopoly of power. In cyber space that's one of the things that we all learn, there's no one nation, no one company, there's no one academic institution that has all the technology, all the talent, all the ability upon which they can move.

The second thing is is the barriers for entry into this domain of cyber space are much different. They're very low and getting increasingly lower and so many can operate in here. And so I would offer that deterrence is a bit different but the idea of being able to impose [inaudible 00:27:07] yes I think that there is something there with regards to that deterrent effect. But I think it's something that we continue to have to work at as we move forward with our forces. Obviously with our whole of nation approach as well.

Gordon Corera: Because this issue of raising costs and deterring it has it's risks as well doesn't it? Because if you respond there are risks of escalation. The US is the most digitally wide of any country therefore in some ways you are the most vulnerable to a cyber attack. It's complicated, isn't it?

Paul Nakasone: So our times are complicated here cyber space is a complicated area but let me come back to the idea of our adversaries right now are operating below a threshold level of war to steal our intellectual property, to steal our PII, to steal our information. They are not looking to raise that level. If you have some type of engagement obviously we believe that that has an effect on us.

Gordon Corera: You contest the space, effectively?

Paul Nakasone: And then I would offer that as you think about that if you do not do that who establishes the norms upon which you operate? It's our adversaries. And so I think that that's one of the areas that I think about as I tend to think about this idea.

Gordon Corera: So that perhaps suggests that hasn't been done ... enough has been done in the past to contest the space day to day with what our adversaries are doing. And that's something you wanna move forward on?

Paul Nakasone: So I would come back to we're a learning force. I think this is part of that. I think this is how that over time that we will adopt, and adapt, and certainly move forward.

Gordon Corera: Lets look a bit ahead a the challenges and the technology of the future. Early on cyber was referred to as another domain of warfare, like land, air, sea, space, but it's different isn't it? Because it's a man made domain, cyber. The technology is constantly changing. The environment of cyberspace is changing. How much of a challenge does that pose to you particularly when, perhaps in the past, America has been able to shape that environment but increasingly other countries, other nations, are shaping it as well?

Paul Nakasone: Partnerships.

Gordon Corera: Partnerships.

Paul Nakasone: Partnerships. Let me talk a little about partnerships because partnerships, for me, really kinda talk about the advent of technology, talent management, all those things that we want to be able to leverage as a force. We talk about partnerships in our national defense strategy about the key piece of that. I would tell you we've learned that in cyber com as well.

What are the partnerships that you're gonna develop with your allies? Industry? Academia? The inter agency? These are partnerships that are incredibly important. I would offer to you that, again, this idea of no one holds the

monopoly on good ideas and technology. The idea that technology is spreading and changing so fast. These partnerships are incredibly important to be able to ensure that you're game is at a very, very high level.

Gordon Corera: What are the technological changes that you think are gonna change the domain of cyber space? Is it 5G? Is it artificial intelligence? What are the things that are on your agenda, or you're looking at thinking this is gonna change my world and the world in which the military operates?

Paul Nakasone: So 5G. Let me begin just on fifth generation. I'm a person that remembers first generation. I was a young Lieutenant and the General had an aide who had this phone that was, of course an analog phone we didn't know that, but it had push buttons and I was like, "Wow that'd be cool to have that." And then by the early 1900s we had second generation. And the neat thing about second generation, of course, is the fact that we could text and the idea of texting. And by the late 1990s we had Smartphones and then of course fourth generation.

We are on the cusp of fifth generation and I am reminded at how much this is gonna change what we do in terms of the speed at the point of end. And so this end point of being able to be at ten gigabits, the idea of being able to instantly download things, these are things that I think will radically change what we're gonna doing. And I would offer that it offers both tremendous opportunities for our nation. Think about how we can change our industry, our medical capabilities, our economy. But it also offers a certain amount of challenge in terms of how do we ensure that this hardware that is being produced is trusted, is able for us to be able to leverage when we want it and have the trusted and verification that it is going to be secure?

Gordon Corera: Because that's one of the challenges which was discussed here at the forum, I think it was yesterday. Was that perhaps it won't just be America building 5G, it may be all the other countries who are building some of that technology. Does that worry you? China particularly?

Paul Nakasone: So I certainly would offer it's something we need to think about. This is so tremendously important. Think about what the Internet means to our economy today and what 5G will do to it in the future. Ensuring that we have a baseline of capability within our nation to produce that hardware and that software, I think, is incredibly important.

Gordon Corera: And China has talked about wanting to become a world leader in the artificial intelligence by 2030 that must worry you as well.

Paul Nakasone: So, again, I think that as with anything we take great credence in what our adversaries are going to say and we watch that. But I would also say that this is a country of innovation. This is a country that has developed the internet. This is a country that has brought the idea of aps, and iPhones, and everything else

that my kids enjoy every single day to the forefront. This is a country that I'll certainly bet on for the future.

Gordon Corera: Yeah it's an interesting point, isn't it? Because America certainly has been in the lead for innovation. I mean Silicone Valley itself was partly built on research for the NSA and the Pentagon and other places. In the '90s you saw Silicone Valley itself kind of take off and, if you like, move ahead of the private sector, moving ahead of government in terms of technological development.

But now you start to see other countries really pushing ahead, particularly China, in terms of their ability to take the lead in some of this technology. How much of a problem is it for you though when it comes to working with Silicone Valley, Silicone Valley is still perhaps nervous about working with you? This is partly a legacy of the Snowden revelations five years ago. There's a nervousness which doesn't clearly exist in China when it comes to their Silicone Valley, their technology companies working. Do you find that? Are you worried about the relationships there?

Paul Nakasone: Partnerships? I come back to the idea of partnerships in terms of we have developed very, very strong partnerships with those in Silicone Valley, those in Austin, those in Boston, a number of different areas. Let me give you an example. In the Army we work very closely with Defense Digital Services. Many of you may have heard of them. They bring tremendous talent to our force to work with our young people. They bring new ideas, they bring fresh insights, they bring a little bit of non military thinking to a very military force. Incredibly important for us because we operate in a domain that changes so rapidly.

I have not experience that. I'd been out to the valley. I've had our soldiers and civilians head out to the valley to talk to different companies. And so I've heard, and certainly I'm aware of the stories in terms of some of the challenges that some have expressed but that's not been the reception that I've received.

Gordon Corera: 'Cause I think there was Google Project Maven, there was this desire not to engage on certain military projects. You've not found that when you've been out there? You've not sensed that nervousness?

Paul Nakasone: So I haven't. I don't think that should mean that we should stop engaging. I think that the most important thing we need to do is engage. That the dialogue that goes on between what we're doing and what the private sector can do is incredibly important. So that they know who Paul Nakasone is and who works for me and others, and understand what we're trying to do. I think that's pretty powerful.

Gordon Corera: And where do you see the cyberspace changing? What's the environment gonna look like in five years? We didn't know how it was gonna look like five years ago today but do you have any sense, or is part of the point you just have to be flexible and adapt?

Paul Nakasone: So I think the latter is really true. So I'm an intelligence officer by training and I would offer that my predictions always haven't been right on.

Gordon Corera: Okay. Do you wanna give me some examples of that, or-

Paul Nakasone: So I-

Gordon Corera: Feel free.

Paul Nakasone: I'll defer on that [inaudible 00:35:23]

Gordon Corera: You're being live streamed but-

Paul Nakasone: But I would offer is I think that many of us, as we take a look at the future one of the things that we do know is that this is a dynamic area. And the most important thing we can do is prepare for that dynamism. So how do we do that? How do we get the right people that we want into our force? How do we encourage those people to stay with us? How do we ensure that we have the right partnerships? How do we take a look at the technologies that are gonna leverage us to a higher readiness? Those are things that I think are much better ways to spend our time than necessarily certain predictions.

Gordon Corera: Lets talk about people then, 'cause you mentioned that. How do you recruit the best people? You cannot compete with the salaries that are being offered on Silicone Valley and there are ... we know that there is a shortage of expertise when it comes to cyber skills.

Paul Nakasone: My experience has been both as the Commander of US Cyber Command and the Director of NSA is we do a tremendous job recruiting people. In our agency this year we're gonna recruit several thousand people to come work with us. We have an attraction that is magnetic and that's the same way in cyber com as well. We do a great job at training that force as well.

Here is where I tell you that we still have a ways to go, and that's the retention piece of it. Okay. This is a challenge, there is no doubt about it because this is a dynamic environment upon which we live. The people that we recruit are very interested in challenges. And when the challenges are there they're most interested in exploring those. But there are other challenges also in the world and so what do we do as a force, whether at the agency or the command, to adapt to that?

I think there's a couple things that we have to do. First of all I would tell you that we have to recognize that there are gradations of talent within our force. I've talked about this before. There's idea of I have people within cyber com today that I would call 50X performers. What's 50X mean? It means that they're fifty times better than their peers. Whether or not that's coding, whether or not that's an om net operator, whether or not that's software developer. They are

so good that they do the work of many. Those are the ones we can't afford to lose. And that goes on the same way with the agency as well. And so what does that mean? We have to think of ways that we can be dynamic enough to ensure that they're interested to stay with our force.

I think the other thing we have to also do is realize that this is probably not gonna be a force that's gonna be like myself that comes in and anticipates doing twenty years, or thirty years and then has a nice retirement and goes off to retirement. This is a dynamic force that comes and goes and I think that we have to recognize that as we move forward.

Gordon Corera: That's a slightly different model isn't it? You mean people will perhaps rotate between the private sector and cyber command in the military and go back and forth and you'll be able to encourage, incentivize, pay them to do that?

Paul Nakasone: So when I go out to the valley one of the things that strikes me is that people change, right? They change different places where they work but they stay in that valley there. It's almost as ... many call it the ecosystem upon which they operate. That's a pretty healthy piece that they're operating within that and that they're doing other things. Why not have that same ecosystem within our government? If they're not going to work within the military maybe it's within the intelligence, maybe it's within the other parts of the inner agency, maybe it's within private sector.

I think the other thing, and it's one of the things that I've done as the director is, I don't think you should ever be afraid to pick up the phone and call those people and say, "Hey how about coming back to the agency? This is a really interesting place to work. We'd like to have you back." It's interesting how much power that has some days.

Gordon Corera: And do you feel that you'll end up looking a bit different from the rest of the military? Maybe you do already. Maybe if you walk around, not you personally, sorry. It wasn't a personal comment. I meant cyber command. If I was to walk around cyber command, I'd love to tomorrow, but would it look different? Would it look different in terms of who's there, the kind of people who are there, from other parts of the military? What would it look like? How diverse is your workforce?

Paul Nakasone: So our workforce is, if you take a loot at it, it's 80% military, it's 20% civilian. The diversity in looks, certainly, but I would offer how about the diversity in thought? I'm more than happy to have the iconoclast that's gonna be in the Army, Navy, Air Force, Marines and says, "Hey sir all I wanna do for the next 20 years is code." "Okay, how good are you?" "I'm really good. I'm a 50X guy." "Okay lets have you."

That's not a model that we necessarily always have. That's something that we've been moving towards in some of the services but I think that's something that

we've gotta accept. If you wanna keep that talent they've gotta do exactly what they wanna do, which is work within this domain.

Gordon Corera: It's gonna look-

PART 2 OF 3 ENDS [00:40:04]

Paul Nakasone: ... exactly what they want to do which is work within this domain.

Gordon Corera: It's going to look different from some of the other commands potentially. It's going to be interesting your relationship with those other commands. When something needs to be done when there's a military mission and you're going to have another command saying, "We could do this with tanks, with airplanes," you could say, "We could do this with cyber." Is that how it's going to be? Are you going to be almost offering something different with different people? Or are you going to be integrated in how you offer solutions to the president and to the joint chiefs?

Paul Nakasone: Yes. I think that in both cases. Already we're looking at how do you integrate this idea of cyber within our war-fighting commands. This comes back to what we've done with Joint Task Force Ares. How do you work with U.S. Central Command under General Joe Votel or U.S. Special Operations Commander General Tony Thomas? We've already started to do that.

But what are the other areas that maybe someday there's some type of capability that Cybercom has that, you're the supported command? You have that type of capability that is important at that time and place of your choosing that the nation wants to leverage. I see that day coming.

Gordon Corera: So it might be if there's a military attack that's about to happen, you might be called on to support that by switching off the air defense or doing something to the other country in preparation for a military strike. That kind of activity.

Paul Nakasone: I would say there's a wide range of activities that we could consider. But I think the important thing here is to think of how best do we utilize this force in defense of the nation? I think that that's where we're really starting to explore our thoughts and how best do we ensure the defense of our nation and the importance of the securing of our nation as well.

Gordon Corera: Okay. I think we've now got some time for questions from the floor, so if you could indicate with your hand. This lady first. Just say briefly who you are. Wait for the microphone, please. Hopefully, there is a microphone coming. Over here we've got mics. Yeah, here comes a mic.

Jane Sherman: I'm Jane Sherman from Bloomfield Hills, Michigan. This may be ... some of this is a little above some of our heads, but I think I've got most of it. But I want to ask you a question. You talked about our enemies are going below the line. I want

to know what's going to bring them above ... could bring them above the line. That's number one. Number two I want to ... and this may be for Department of Homeland Security. But what are we doing to stop the social media creating terrorism, terrorist groups, etc. etc., that's been rampant throughout the world and I know it is here. Is that for Homeland Security or is that in your department?

Paul Nakasone: I'm going to take the latter first. I would say the Deputy Attorney General this week really hit it on the head as he talked about the different ways that we're looking at malign influence operations. I think going back to his piece is spot on. He's done a very good job in outlining how we're going to go forward. Above the threshold of war. I would offer if a nation state decided to attack our infrastructure. I would say that's above the threshold level of war. And we would certainly respond. That would be an example of where I would anticipate that policy decision would be made and certainly we would react.

Gordon Corera: But interfering in election wouldn't be seen necessarily as that level. That's where it gets interesting, isn't it?

Paul Nakasone: Again, these are policy decisions upon which our national leaders decide. Again, I think the important thing for us is what are the options that we can present to those policymakers in the future.

Gordon Corera: I've got a question here from the gentleman in the front. Microphone is on its way.

Speaker 1: First, general thanks for coming out here and speaking to us. You've said that your mission is protect the network, protect the data, protect the weapon system. In my previous job, I was one of the chief buyers of weapon system. One of the things that worried me was cyber-attack on our weapon systems. How do you protect a DDG, the scale of a DDG? An F35 which is a bucket of flying software that happens to drop ordnance. A Patriot battery which spoofing of a Patriot battery could have devastating effects. Could you address protection of the weapon system?

Paul Nakasone: I think it begins with baking that security in as opposed to an afterthought, right? As we design these systems, how do we ensure that we've thought about the security not only from external attacks but also from the idea of an internal attack like cyber? I think the second piece is that these are systems that operate on networks. One of the most effective things we do on networks is to continue to hunt on networks. So we should never be satisfied with the idea that our adversaries aren't trying to penetrate our weapon systems and our networks.

And the thing that I would say is that we continue to ensure that we've got optimal intelligence of what our adversaries are trying to do. Those are three ways that I'd offer that are really important ways upon which we defend our weapon systems.

Gordon Corera: And got to look after the supply chain.

Paul Nakasone: Certainly.

Gordon Corera: It's increasingly important isn't it in cyber?

Paul Nakasone: Certainly. Again, I come back to this idea of the perspective of thinking about the security of the weapon system before it's even designed. I think that's critical as we think about the future.

Gordon Corera: Right here.

Dina Temple: Hi, Dina Temple with National Public Radio. When we talk about offensive cyber a lot of times we talk about what's called a cyber-bomb. Could you explain exactly what a cyber-bomb is and perhaps give us an example of how it would work?

Paul Nakasone: No. And I don't mean to be glib about that, but I would offer that I'm not really understanding of what a cyber-bomb is. Here's what I do understand. There are a number of different actions that we certainly do upon which we can create outcomes on our adversaries. And that's everything from exploit that adversary, to disrupt that adversary, to conduct operations to destroy their physical hardware or their software. And I think that's probably more of the language that I would use. But thank you very much.

Gordon Corera: Gentleman here.

David Sanger: General David Sanger from the New York Times. Thank you very much for coming out to do this today. I wanted to press you a little bit on the persistent engagement concept that you had here. I've talked to people in and out of cyber command others who think about this. They're trying to get their heads around the question of how this differs from traditional preemption and what the risks would be.

So, try this question by example. If you went into an adversary network. China, Russia, name whatever country it would be. And you thought you saw an attack amassing that you wanted to go at preemptively because as you've said, by the time it comes here it's too late. First of all, would you still always require presidential authorization? Because persistent engagement would mean moving pretty quickly. And secondly, do you have a risk that as soon as you act first ... of course the other country is going to say, "We weren't getting ready to attack you. You just attacked a group of people who were putting together educational software for kindergartners or something." You'd have a very difficult time proving the opposite at least in public even if you were convinced.

Talk us a little bit through the risks of escalation here.

Paul Nakasone: So I'd offer with anything, any operation that our military forces do, first of all, there's going to be authorities upon which they operate. Right? So, however, those authorities are done, whether or not it's in cyber or on the ground or in the sea, commanders are going to operate based upon those authorities and move forward on that.

The second thing that's always going to be done is deconfliction. So we're going to deconflict in terms of the targets that we're looking at. In terms of preemption versus persistent engagement, my idea I would offer as we look at division, so one of the things is that we are constantly engaged. It's not just an offensive engagement, but it's also a defensive engagement as well.

In terms of the targets that we might engage, I think that that's obviously one of the areas that would be a broader discussion in terms of what has the impact. What do we want to send a message to our adversaries? What is certainly a target that is both lawful and is one that we would want to engage? So, these are obviously questions and elements that would be involved in this idea of persistent engagement. But it's something that I think that we are looking at very, very carefully and one that I think has a lot of merit as we move forward. Particularly as we look at such things as where malware is placed. Or what our adversaries may be doing upon which they may be stealing our intellectual property.

These are all areas that I think offer some ideas that persistent engagement may actually have some merit.

Ian Murta: Hi, my name's Ian Murta raised in Aspen, Colorado. I just wanted to ask how do you keep up with the technology? It's constantly evolving and constantly changing. It seems like every other day something new comes out. I just wanted to figure out how you kept up with that.

Paul Nakasone: We hire the best and the brightest. That's truly the most important thing that we do are the people that understand the technology. That develop the technology. That have the partnerships to leverage the technology. That's the piece that we often don't talk enough about in cyberspace is the human element. Those people are the ones that understand it best that give us the greatest ideas, that develop that technology. That is the component that makes us different I would offer.

Dan Porterfield: My name is Gary Davis, Aspen, Colorado. How do you work with Homeland Security in terms of the domestic economy ... the domestic situation both in terms of organized groups and rogue lone warriors? Is there an overlap or duplication? Is it efficient?

Paul Nakasone: We work closely through Department of Homeland Security with our sector-specific agents. So as we take a look at the different critical infrastructure elements throughout our nation of which there are 17. We partner very closely

with DHS and that sector-specific agency that has the requirements. Let me give you an example.

Finance. As we take a look at the financial industry, we not only partner with Department of Homeland Security but also the Department of Treasury. Again, the lead for this is Department of Homeland Security. The idea of this close partnership is something that is really etched in us and one of the things that I think we have done a lot to work over the past couple of years.

Is it duplicative? No, I think it's one of the things that I would offer that we continue to work at every single day to improve those partnerships. And I would say that's one of the things that we have learned over the past several years is that protection is only as good as the partnership that we develop.

Andrew Weiss: Hi, General, thanks so much for your service and for doing this. I'm Andrew Weiss from the Carnegie Endowment in Washington. When we look at what happened with Russia in 2016, at the end of his presidency President Obama came out and basically something to the effect of we need to be mindful of the dangers of escalation. He didn't exactly say this but a cyber expert said to me, we have the sharpest rocks but we live in the glassiest house.

I'm sort of curious when you look at an adversary like Russia which has a society that's far less digitized, what is our relative advantage in confronting an adversary which sees escalation, audacity, lack of embarrassment as it's key attributes?

Paul Nakasone: I come back again, I think that as we think about strategic engagement and the idea of the adversaries that we must focus on early on and into the future and that's Russia and China. I would offer that we have to have some manner upon which we're going to look at being able to contest them in places like cyberspace. If we don't, if we decide that we're going to stand on the sidelines, that we're not going to bring the powers of our nation against our adversaries in cyberspace and that's more than just cyber, right? It's the whole capabilities that our nation has. I think again that we run the risk of our adversaries defining what they're going to do in this domain.

And so I certainly understand that these are decisions and certainly discussions that have to take place in terms of what's the cost benefit. But that discussion I think has to take place and that discussion also has to take place with the idea of are we going to contest our adversaries in this new domain?

Gordon Corera: Contesting them does risk escalation. That's the risk that's in there when you're doing that cost-benefit analysis.

Paul Nakasone: So it could. But, may not. Maybe our adversaries do not want to escalate. Maybe that they want to use cyberspace in terms of, again, being lower than the threshold of armed conflict. But again my concern is that if we do not bring

the elements of our nation's power against our adversaries in this space, if we don't decide that contesting them or engaging them is important, then I think our adversaries have a much easier time of defining what they are going to do.

Gordon Corera: Okay, we're nearly out of time, but I've got time for just a couple of questions. One here.

Courtney Kube: Thank you. That's okay. Courtney Kube from NBC News. We had DNI Coats here a couple of days ago and one of the things he said was that the U.S. has to be relentless in terms of calling out the Russians for what they're doing. A couple of months ago at a forum, the Deputy Director Operations for the NSC ... or NSA I'm sorry, said that the U.S. does not have the political fortitude to say how we'll strike back yet against Russian influence operations.

Do you agree with that? Have you seen any change in that? That the U.S. may actually start calling out the Russians and talking about how they'll respond?

Paul Nakasone: I'm not familiar with the person at the National Security Agency that offered that comment. But I would offer, here's what I would say. We have to as a nation bring all of the elements of our power together against our adversaries. So whether it's in the information sphere, the economic sphere, the military sphere, we have to address our adversaries with the combined weight of what we have. We have a tremendous amount of combined weight with our capabilities.

So, I think that's the best way that I would offer a response that certainly I think it's among the most important things that we do.

Gordon Corera: I think I've got one question here.

Hank Jurokovich: My name's Hank Jurokovich. General, it's great to hear your views. Let me see. Multiple hats come with multiple bosses, so two months into your new job, how's that going?

Paul Nakasone: I guess the first way I could say it is you could probably ask my bosses. My perspective is it's going really well. In all seriousness here's what I would say is that I get great guidance from the Secretary of Defense, the Director of National Intelligence. I have tremendous people that work with me and for me. It's not hard for me to understand what their guidance is. And I've been able to do that at least over the past 70 days and I really appreciate the steerage that they've given me and certainly the work that my folks have done, so thanks.

Gordon Corera: And it's true isn't it that the two hats could be separated. That's one of the things that's being looked at under a review. But you'd still have to work very closely with NSA Cyber Command, wouldn't it? If that was the outcome.

Paul Nakasone: Certainly predecisional but, whatever decision is made, the partnership between the National Security Agency and U.S. Cyber Command is going to be one that is critically important to our nation. So whether or not it's one person or two people, that partnership I would offer is the most important thing that we should think about.

Gordon Corera: Okay, I think we have time for one more question.

Turner Holcomb: Thank you, General. Thank you as well. I was hoping to see a tie today. But my question ... My name is Turner Holcomb. I'm a cadet from the U.S. Air Force Academy and my question has to do with the future of warfare being a hybrid type where we not only worry about deterrence with near-peer competitors but also the threat of violent extremist organizations. What do you do to prepare for both of those threats?

Paul Nakasone: I would offer the lesson that I've learned over my career is that you train the best people to be the best leaders to operate in a variety of different domains. For the past 17 years, our nation has I would offer, done incredible work against violent extremist organizations. Take a look at what the intelligence community, what our operational forces have done to collect information. To analyze that information. To provide that information forward to ensure the protection of our forces and the security of our nation.

Incredible amount of work. I would offer from a person that was at the Pentagon on 911, that has been a tremendous learning experience for all of us. And so the future in terms of how we're going to address these different threats, the one constant we'll have and the one constant that will be successful is really great people. So, thank you very much.

Gordon Corera: Thank you very much. It just needs for me to say thank you all for coming. Thank you for attending a wonderful forum. Thank you for the organizers for doing it. And thank you above all for General Nakasone for giving us such a great ending to this forum. Thank you.

PART 3 OF 3 ENDS [00:58:08]